

# Verification of Declaration of Adherence

Declaring Company: Google LLC



EU  
CLOUD  
COC

**Verification-ID** 2020LVL02SCOPE015

**Date of Approval** December 2023

**Valid until** December 2024

## Table of Contents

<b>1</b>	<b>Verification against v2.11 of the EU Cloud CoC</b>	<b>3</b>
<b>2</b>	<b>List of declared services</b>	<b>3</b>
2.1	Google Workspace	3
2.2	Google Cloud Platform	4
<b>3</b>	<b>Verification Process - Background</b>	<b>6</b>
3.1	Approval of the Code and Accreditation of the Monitoring Body	6
3.2	Principles of the Verification Process	6
3.3	Multiple Safeguards of Compliance	7
3.4	Process in Detail	7
3.4.1	Levels of Compliance	8
3.4.2	Final decision on the applicable Level of Compliance	9
3.5	Transparency about adherence	9
<b>4</b>	<b>Assessment of declared services by Google (see 2.)</b>	<b>10</b>
4.1	Fact Finding	10
4.2	Selection of Controls for in-depth assessment	10
4.3	Examined Controls and related findings by the Monitoring Body	11
4.3.1	Examined Controls	11
4.3.2	Findings by the Monitoring Body	11
<b>5</b>	<b>Conclusion</b>	<b>13</b>
<b>6</b>	<b>Validity</b>	<b>13</b>

## 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'**)<sup>1</sup> in its version 2.11 (**'v2.11'**)<sup>2</sup> as of December 2020.

Originally drafted by the Cloud Select Industry Group<sup>3</sup> (**'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<sup>4</sup> 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'**)<sup>5</sup>.

## 2 List of declared services

### 2.1 Google Workspace<sup>6</sup>

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.<sup>7</sup>

- Admin Console
- Assignments
- Classroom
- Cloud Identity
- Cloud Search
- 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
- Google Slides
- Google Tasks
- Google Vault
- Google Voice

---

<sup>1</sup> <https://eucoc.cloud>

<sup>2</sup> <https://eucoc.cloud/get-the-code>

<sup>3</sup> <https://ec.europa.eu/digital-single-market/en/cloud-select-industry-group-code-conduct>

<sup>4</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046>

<sup>5</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679>

<sup>6</sup> <https://workspace.google.com/>

<sup>7</sup> **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 Workspace Migrate
- Mobile Device Management

## 2.2 Google Cloud Platform<sup>8</sup>

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.<sup>9</sup>

- Access Approval
- Access Context Manager
- Access Transparency
- Agent Assist
- AI Platform Data Labeling
- AI Platform Neural Architecture Search (NAS)
- AI Platform Training and Prediction
- AlloyDB
- Anthos Config Management
- Anthos Identity Service
- Anthos Service Mesh
- API Gateway
- Apigee
- App Engine
- Artifact Registry
- Assured Workloads
- AutoML Natural Language
- AutoML Tables
- AutoML Translation
- AutoML Video
- AutoML Vision
- Backup for GKE
- Batch
- BeyondCorp Enterprise
- BigQuery
- BigQuery Data Transfer Service
- Binary Authorization
- CCAI Platform
- Certificate Authority Service
- Chronicle SIEM
- Cloud Asset Inventory
- Cloud Bigtable
- Cloud Build
- Cloud CDN
- Cloud Composer
- Cloud Data Fusion
- Cloud Data Loss Prevention
- 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 Intrusion Detection System)
- Cloud Interconnect

---

<sup>8</sup> <https://cloud.google.com/>

<sup>9</sup> **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 Key Management Service
- Cloud Life Sciences (formerly Google Genomics)
- 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 for Firebase
- Cloud Tasks
- Cloud Trace
- Cloud Translation
- Cloud Vision
- Cloud VPN
- Compute Engine
- Connect
- Contact Center AI (CCAI)
- Container Registry
- Data Catalog
- Database Migration Service
- Dataflow
- Dataplex
- Dataproc
- Dataproc Metastore
- Datastore
- Dialogflow
- Discovery Solutions
- Document AI
- Document AI Warehouse
- Duet AI on Cloud Serving Stack
- Eventarc
- Firebase Authentication
- Firebase Test Lab
- Firestore
- Gen App Builder - Enterprise Search
- Generative AI App Builder
- Generative AI Support on Vertex AI
- Google Cloud Armor
- Google Cloud Deploy
- Google Cloud Identity-Aware Proxy
- Google Cloud Storage
- Google Cloud Threat Intelligence for Chronicle
- Google Kubernetes Engine
- Healthcare Data Engine (HDE)
- Hub
- Identity & Access Management (IAM)
- Identity Platform
- IoT Core
- Key Access Justifications (KAJ)
- Looker Studio
- Managed Service for Microsoft Active Directory (AD)
- Memorystore
- Migrate for Compute Engine
- 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
- Security Command Center
- Service Directory
- Service Infrastructure
- 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
- 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<sup>10</sup>.

#### 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<sup>11</sup>.

The Code has been officially approved in May 2021<sup>12</sup>. SCOPE Europe has been officially accredited as Monitoring Body in May 2021<sup>13</sup>. 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.<sup>14</sup>

#### 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.

---

<sup>10</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679>

<sup>11</sup> <https://scope-europe.eu>

<sup>12</sup> <https://www.gegevensbeschermingsautoriteit.be/publications/decision-n05-2021-of-20-may-2021.pdf>

<sup>13</sup> <https://www.gegevensbeschermingsautoriteit.be/publications/decision-n-06-2021-of-20-may-2021.pdf>

<sup>14</sup> <https://euoc.cloud/en/public-register/assessment-procedure/>

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 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<sup>15</sup> and referring to the Public Register of the EU Cloud CoC<sup>16</sup> to enable Customers to verify the validity of adherence.

---

<sup>15</sup> <https://euococ.cloud/en/public-register/levels-of-compliance/>

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

## 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<sup>17</sup>, 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 Cloud 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<sup>18</sup>, the Monitoring Body analysed the responses and information provided by Google.

Google's declared services have been externally certified and audited. Google holds an ISO/IEC 27001:2013, certificate, 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/IEC 27001:2013, 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.

---

<sup>17</sup> You can access the Verification Report(s) of previous year(s) via the following link(s): [Google Verification Report \(2022\)](#)

<sup>18</sup> <https://eucoc.cloud/en/about/about-eu-cloud-coc/applicable-procedures/>

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 review were: 5.1.A, 5.1.C, 5.1.E, 5.1.F, 5.1.H, 5.2.A, 5.2.C, 5.3.B, 5.3.D, 5.3.E, 5.4.A, 5.4.C, 5.4.E, 5.4.F, 5.5.A-E, 5.7.B, 5.7.E, 5.7.F, 5.8.A, 5.12.B, 5.12.G, 5.13.A, 5.13.B, 5.14.A, 5.14.C, 5.14.F, 6.1.A, 6.1.C and 6.2.P.

### 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.

The Monitoring Body focused on the assistance provided to the Customers. In accordance with the information provided by Google, Customers are provided with self-service capabilities to individually manage the data subject rights requests. Additionally, multiple communication channels are put in place for Customers to be able to request additional assistance, including contact channels provided in the Cloud Data Processing Addendum (CDPA) and more specific channels such as Customer portals, inquiry forms and contact requests through self-service functionalities are made available to Customers. Moreover, Customers are provided with various self-service information and recourses via Google's Privacy Resource Center, offering information about the provided services, in addition to more specific whitepapers.

Customers' Audit Rights were also assessed by the Monitoring Body. Google's contractual documents confirmed that it makes available third-party audit reports and certificates to the Customers. Additional evidence of compliance to data protection laws may be requested via dedicated communication channels mentioned above. Further, Customers are enabled to request individual audits and Customer Audit Rights are included as standard part of the CDPA. In addition to this, Google has provided Monitoring Body with an overview of the methodology to determine the costs of an audit and indicated that audit costs, if applicable, are communicated to the Customers before execution of any audit activities.

Additionally, Google indicated that it provides support to Customers with the performance of Data Protection Impact Assessment (DPIA) by means of making available relevant information via its Privacy Resource Center and put in place dedicated communication channels for Customer inquiries in relation to data protection to fulfil this contractual obligation. In the same vein, Google provides information regarding implemented technical and organizational measures in its CDPA, as well as via Security Whitepapers and dedicated web pages.

The data breach procedures have also been assessed by the Monitoring Body. Google indicated that relevant Incident Response Management procedures and Data Breach response procedures are in place in order to identify, document, and remediate incidents which could impact the availability, confidentiality, security or data protection of the Customer Personal Data. Additionally, incident notification is included as a standard part of the CDPA.

Another area of the assessment has been subprocessors management process. Google's contractual obligations ensures that subprocessors only access and use Customer Personal Data to the extent required to perform its obligations, and that the same data protection measures and appropriate technical and organisational measures, as provided by the CDPA are flown down to its subprocessors. Moreover, before onboarding subprocessors, the latter undergo an audit of the security and privacy practices, which is performed by Google.

Finally, third country transfers have been assessed. Google has confirmed that it relies on the adequacy decisions and the Standard Contractual Clauses (SCCs). Additionally, Google indicated that it relies on the EU-U.S. Data Privacy Framework ('DPF') as an Alternative Transfer Solution under the CDPA for the transfers of Customer Personal Data to the United States. Adequacy decisions are monitored to ensure their relevancy.

## 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<sup>19</sup> 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<sup>20</sup>.

**Verification-date:** December 2023

**Valid until:** December 2024

**Verification-ID:** 2020LVL02SCOPE015

---

<sup>19</sup> <https://eucooc.cloud/en/public-register/>

<sup>20</sup> <https://eucooc.cloud/en/public-register/>