SCOPE EUROPE

Verification of Declaration of Adherence

Declaring Company: Google LLC

Verification-ID	2020PV02SCOPE015
Date of Approval	December 2020
Due date of Approval	December 2021

Table of Contents

1 Verification against v2.6 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 2.6 (**'v2.6'**)[2] as of March 2019.

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 v2.6 and its provisions has been aligned to the European General Data Protection Regulation (**'GDPR'**)[5].

The EU Cloud CoC already applies the same principles and procedures now, pending the endorsement of the Code and its official approval by supervisory authorities, cloud service providers are welcomed and invited to sign up their services under v2.6 of the EU Cloud CoC, to publicly underpin their efforts to comply with GDPR requirements.

2 List of declared services

2.1 Google Cloud Platform[6]

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.

Access Context Manager
Access Transparency
AI Platform Notebooks
AI Platform Training and Prediction
App Engine
AutoML Natural Language
AutoML Tables
AutoML Translation
AutoML Video
AutoML Vision
BigQuery
BigQuery Data Transfer Service
Cloud Bigtable
Cloud Billing API
Cloud Build
Cloud CDN
Cloud Data Fusion
Cloud Data Loss Prevention

[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://cloud.google.com/gcp

Cloud Deployment Manager
Cloud DNS
Cloud Endpoints
Cloud Filestore
Cloud Functions
Cloud Functions for Firebase
Cloud Healthcare
Cloud HSM
Cloud Interconnect
Cloud Key Management Service
Cloud Life Sciences (formerly Google Genomics)
Cloud Load Balancing
Cloud NAT (Network Address Translation)
Cloud Natural Language API
Cloud Router
Cloud Run (fully managed)
Cloud Source Repositories
Cloud Spanner
Cloud SQL
Cloud Storage
Cloud Storage for Firebase
Cloud Translation
Cloud Vision
Cloud VPN
Compute Engine
Container Registry
Dataflow
Datalab
Dataproc
Datastore
Data Catalog
Dialogflow
Firebase Authentication
Firebase Test Lab
Firestore
Google Cloud Armor
Google Cloud Identity-Aware Proxy
Google Kubernetes Engine
Identity & Access Management (IAM)
IoT Core
Memorystore
Network Service Tiers
Persistent Disk
Pub/Sub
Resource Manager API
Service Control
Service Consumer Management
Service Management
Speech-to-Text
Stackdriver Debugger
Stackdriver Error Reporting
Stackdriver Logging
Stackdriver Profiler
Stackdriver Trace
Storage Transfer Service
Talent Solution
Text-to-Speech
Video Intelligence API
VPC Service Controls
Virtual Private Cloud
Web Security Scanner

2.2 Google Workspace[7]

Google Workspace[8] 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

Admin Console
Calendar
Classroom
Cloud Identity
Cloud Search
Contacts
Docs
Drive
Forms
Gmail
Google+ (or Currents)
Groups
Hangouts
Hangouts Chat (or Google Chat)
Hangouts Meet (or Google Meet)
Jamboard
Keep
Mobile Device Management*
Sheets
Sites
Slides
Tasks
Vault
Voice

3 Verification Process - Background

V2.6 of the EU Cloud CoC has been developed against GDPR and hence provides mechanisms as required by Articles 40 and 41 GDPR[9]. Those mechanisms will apply pending the formal approval of the EU Cloud CoC and accreditation of the Monitoring Body.

3.1 Provisional Status of the Verification Process

The services concerned passed a provisional verification process by the Monitoring Body of the EU Cloud CoC, i.e. SCOPE Europe sprl/bvba[10].

[7] https://workspace.google.com/
[8] The assessment started whilst Cloud Services were listed as "G Suite". During the process of verification the brand was renamed to "Google Workspace". Google assured that besides there have not been any material changes besides the brand name, so that the Monitoring Body could transfer its assessment results. To properly reflect the current brand names, the report refers to Google Workspace.
[9] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679
[10] https://scope-europe.eu

This provisional verification process follows the same principles and procedures as the EU Cloud CoC will apply under its official approval and accreditation. 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.[11]

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 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.

[11] 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 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

V2.6 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 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.

3.5 Transparency about adherence

Each service adherent to the EU Cloud CoC must transparently communicate its adherence by both using the appropriate Compliance Mark[12] and refer to the Public Register of the EU Cloud CoC[13] to enable Customers to verify the validity of adherence.

4 Assessment of declared services by Google (see 0.)

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. 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.

Google promptly responded within the template. 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. Google provided information illustrating the actual structure of the services declared adherent and describing the technical and contractual framework. Google provided convincing responses that, as all services declared adherent are either part of the "Google Cloud Platform" or "Google Workspace", all declared services sit on top of Google Common Infrastructure and share to the extent relevant for the Code the same contractual framework.

4.2 Selection of Controls for in-depth assessment

Following the provisions of the Code and the Assessment Procedure applicable to the EU Cloud CoC[14], the Monitoring Body analysed the responses and information provided by Google.

---

[12] https://eucoc.cloud/en/public-register/levels-of-compliance/
[13] https://eucoc.cloud/en/public-register/
[14] https://eucoc.cloud/en/about/about-eu-cloud-coc/applicable-procedures/

Google declared cloud services subject to this declaration of adherence[15] have been externally certified and audited, e.g. Google holds current ISO 27001 certificates. Notwithstanding other certifications[16], 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.

The Monitoring Body did also take into account relevant publications, e.g. of supervisory authorities, related to the declared Cloud Services and, accordingly, focused in the in-depth assessment also on requirements when engaging subprocessors as well as the termination of the Cloud Services Agreement, including retention periods.

Another area decided to be of relevance for the Initial Assessment has been third country transfers and whether measures regarding safeguards of such transfers are implemented accordingly, also taking into account that the European Court of Justice issued its decision in the so-called "Schrems II" ruling during the period in which the Cloud Services were assessed.

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 of the requirements of the Code were met by Google 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. The controls selected for this level of review were:

5.1.D, 5.1.E, 5.1.I, 5.2.C, 5.3.A, 5.3.B, 5.3.E, 5.3.F, 5.4.C, 5.4.D, 5.4.E, 5.5.D, 5.7.B, 5.9.B, 5.11.B, 5.12.B, 5.12.C, 5.12.D, 5.12.E, 5.12.E, 5.14.F, 6.1.A.

Additionally, samples were requested regarding Controls: 5.5.C, 5.8.A, 5.12.A.

Based on the information provided by Google, a follow-up request was made, for further detail on implemented measures related to Controls and respective information provided for: 5.3.A, 5.4.E, 5.5.C, 5.7.B, 5.11.B, 5.12.A, 6.1.A.

[15] As listed above in section 2
[16] https://cloud.google.com/security/compliance/offerings

4.3.2 Findings by the Monitoring Body

During the process of verification, Google consistently gave the 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 Google confirmed that all Cloud Services being declared in this declaration of adherence are covered by the respective certificates.

Considering the amount of Cloud Services declared adherent and the relevance of subprocessing in this context, the Monitoring Body, in its assessment, chose to focus on verifying that Cloud Services declared adherent meet all requirements related to engaging subprocessors. The Code requires that a CSP obtains written authorization of the Customer prior to the processing of Customer Personal Data when engaging subprocessors. Such authorization may be either specific or general. A general authorization is considered, where a Cloud Service Provider, subject to the Cloud Service Agreement, can perform any changes to engaged subprocessors without being required to obtain explicit authorization provided that any such change will be duly notified. Google referred to the agreements in place, ensuring that Customers will know the subprocessors in place when signing the Cloud Service Agreement and thus will be able to determine any future modifications. Per requested clarification of the Monitoring Body, Google convincingly responded that also Google affiliates, at the time of entering into the agreement, are available and communicated to the Customer. Google also provided convincing responses ensuring that any changes to Google affiliates involved in subprocessing are subject to the overall sub-processor change notification procedures. Regarding Customer notification, the Code allows for a variety of suitable means, including but not limited to a communication via websites, dashboards but also email notifications. Related to the obligations related to changes to engaged subprocessors, Google clarified that Customer will be notified at least 30 days before any such change applies. To the extent such changes relate to third party subprocessors Customers will also be notified via email.

The Monitoring Body assessed whether measures regarding safeguards of third country transfers were implemented accordingly, especially as the European Court of Justice issued its decision in the so-called “Schrems II” ruling during the period in which the Cloud Services were assessed. Google sufficiently and convincingly reported how Customers were notified about changes related to the so-called “Schrems II” ruling, including informing Customers on Google 's commitment to EU international data transfers in a dedicated blog post and by sending communication to Customers regarding changes made to contractual and data processing terms. Google also reported that Customers were informed that transfers of personal data are no longer safeguarded solely with the EU-U.S. Privacy Shield, but other means such as Standard Contractual Clauses. Furthermore, Google‘s responses convincingly assured that (at the time of the assessment), Google did not receive any official request from a Supervisory Authority to suspend data transfers, and agreed to provide notification to the Monitoring Body if if Google receives any such request.

The Monitoring Body assessed in more detail two requirements which are related to confidentiality requirements. First, requirements related to the confidentiality of the processing were verified as the confidentiality template agreement was assessed, verifying that provisions related to appropriate confidentiality obligations for employees prior, during and after engaging in relevant data processing activities are met. Second, a sample was requested to ensure that Google maintains an up-to-date and accurate record of all activities carried out on behalf of the Customer containing all required information according to Article 30.2 GDPR. As Google’s records of processing are documented and stored internally with restricted access consistent with internal security and privacy policies. Google explained and illustrated in a dedicated web conference via screen sharing the existence of such records and the means how to dynamically retrieve up-to-date records of processing if and to the extent necessary. Related follow-up questions during the web conference on the subject matter were answered sufficiently and convincingly.

The Monitoring assessed the requirements related to data retention. Google provided evidence that Customer Personal Data will be deleted (either as requested by Customer or upon termination) in due time within a maximum period of 180 days. Per requested clarification of the Monitoring Body, Google confirmed, also referencing internal policies, that the maximum period of 180 days is related to backups , stating the deletion of data from active systems takes about two months and that the 180 days period refers to data center backups. The provided schedule appears reasonable from a Monitoring Body’s perspective. First, data processed is of highest importance to Customers, requiring highest standards regarding business continuity. Second, terms being accepted by supervisory authorities only refer to the terminology “in due time”; transparently communicating the given 180 days period

determines a precise maximum timeframe without any room for interpretation, and thus enabling Customers to effectively enforce requested deletions.

5 Conclusion

Given answers 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[17] alongside this report.

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 2020 **Valid until**: December 2021

Verification-ID: 2020PV02SCOPE015

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