SCOPE EUROPE

Verification of Declaration of Adherence

Declaring Company: Alibaba Cloud (Singapore) Private Limited

EU CLOUD COC

Verification-ID	2020LVL02SCOPE013
Date of Approval	June 2021
Valid until	June 2022

Table of Contents

1 Verification against v2.11 of the EU Cloud CoC

This Declaration of Adherence was against the *European Data Protection Code of Conduct for Cloud Service Providers* (**'EU Cloud CoC'**)[1] in its version 2.11 (**'v2.11'**)[2] as of December 2020.

Originally being drafted by the Cloud Select Industry Group[3] (**'C-SIG'**) the EU Cloud CoC, at that time being called C-SIG Code of Conduct on data protection for Cloud Service Providers, the Code was developed against Directive 95/46/EC[4] incorporates feedback by the European Commission as well as Working Party 29. Following an extensive revision of earlier versions of Code and further developing the substance of the Code v2.11 and its provisions has been aligned to the European General Data Protection Regulation (**'GDPR'**)[5].

2 List of declared services

2.1 Alibaba Cloud products and services

Alibaba Cloud, a business unit of Alibaba Group, provides a comprehensive suite of global cloud computing services to their global customers and partners as well as Alibaba Cloud's own e-commerce ecosystem. The cloud services provided by Alibaba Cloud are powered by self-developed cloud services platform and technologies. Alibaba Cloud aims to turn cloud computing into a state-of-the-art computing infrastructure by investing heavily in technical innovation to continually improve the computing capabilities and economies of scale of its services.[6]

2.1.1 Elastic Computing

- Elastic Compute Service ("ECS")
- Simple Application Server
- Elastic GPU Service
- Auto Scaling
- Server Load Balancer
- Resource Orchestration Service
- E-HPC
- ECS Bare Metal Instance
- Super Computing Cluster
- Function Compute
- Batch Compute
- Dedicated Host
- Operation Orchestration Service

[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.

2.1.2 Networking & CDN

- Content Delivery Network ("CDN")
- Dynamic Content Delivery Network ("DCDN")
- Server Load Balancer ("SLB")
- Virtual Private Cloud ("VPC")
- Express Connect
- Elastic IP
- VPN Gateway
- NAT Gateway
- Cloud Enterprise Network ("CEN")
- Smart Access Gateway
- Data Transfer Plan
- Alibaba Cloud PrivateZone

2.1.3 Database

- ApsaraDB for OceanBase
- Relational Database Service ("RDS")
- ApsaraDB for Redis
- ApsaraDB RDS for MySQL
- ApsaraDB RDS for SQL Server
- ApsaraDB RDS for PostgreSQL
- ApsaraDB RDS for PPAS
- ApsaraDB for MongoDB
- ApsaraDB for Memcache
- Data Transmission Service
- AnalyticDB for PostgreSQL
- Distributed Relational Database Service ("DRDS")
- Time Series Database ("TSDB")
- ApsaraDB for MariaDB TX
- Database Backup
- Data Management
- Data Lake Analytics
- ApsaraDB for POLARDB

2.1.4 Storage

- Table Store
- Network Attached Storage
- Hybrid Cloud Storage Array
- Data Transport
- Hybrid Backup Recovery
- Cloud Storage Gateway
- Object Storage Service ("OSS")
- Apsara File Storage NAS
- Elastic Block Storage

2.1.5 Security

- Anti-DDoS Basic
- Anti-DDoS
- Cloud Firewall
- Web Application Firewall
- Server Guard
- Alibaba Cloud SSL Certificates Service
- Website Threat Inspector
- Managed Security Service
- Content Moderation
- Anti-Bot Service
- Security Center
- GameShield
- Bastionhost
- Data Encryption Service
- Identity as a service ("IDaaS")
- Sensitive Data Discovery and Protection ("SDDP")
- CloudMonitor
- Key Management Service

2.1.6 Enterprise Applications & Cloud Communication

- Web Hosting
- Domains
- Alibaba Cloud DNS
- Ding Talk
- Short Message Service (SMS)

2.1.7 Analytics

- E-MapReduce
- MaxCompute
- DataWorks
- Data Integration
- Quick BI
- DataV
- Intelligent Robot
- Dataphin
- Alibaba Cloud Elasticsearch
- Realtime Compute for Apache Flink
- Message Service
- API Gateway
- Log Service
- Direct Mail
- Blockchain as a Service
- Enterprise Email

2.1.8 Artificial Intelligence

- Image Search
- Machine Learning Platform For AI
- Machine Translation
- Intelligent Speech Interaction

2.1.9 Media Services

- ApsaraVideo Live
- ApsaraVideo Media Processing
- ApsaraVideo VOD

2.1.10 Container & Middleware

- Elastic Container Instance
- Container Service for Kubernetes (ACK)
- Container Registry
- Alibaba Cloud Service Mesh
- Enterprise Distributed Application Service
- Message Queue
- Application Configuration Management
- Tracing Analysis
- Application Real-Time Monitoring Service
- Application High Availability Service
- AliwareMQ for IoT
- AlibabaMQ for Apache Kafka
- AlibabaMQ for Apache RocketMQ

2.1.11 Developer Services

- Cloud Shell
- ActionTrail
- OpenAPI Explorer
- Resource Access Management
- Cloud Config

2.1.12 Internet of Things

- Alibaba Cloud Link IoT Platform
- Alibaba Cloud Link ID[2]

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[7].

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[8].

The Code has been officially approved May 2021[9]. SCOPE Europe has been officially accredited as Monitoring Body May 2021[10]. 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.

---

[7] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679
[8] https://scope-europe.eu
[9] https://www.gegevensbeschermingsautoriteit.be/publications/decision-n05-2021-of-20-may-2021.pdf
[10] https://www.gegevensbeschermingsautoriteit.be/publications/decision-n-06-2021-of-20-may-2021.pdf
[11] https://eucoc.cloud/en/public-register/assessment-procedure/

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.

The CSP may do so either by referencing existing third-party audits or certifications and their respective reports or by free text. Additionally, the CSP will have to provide a general overview on the functionalities, technical and organizational and contractual frameworks of the service(s) declared adherent.

With regards to internationally recognized standards, the Monitoring Body will consider the mapping as provided by the Controls Catalogue. However, the Monitoring Body will verify whether (a) any third-party certification or audit provided by the CSP applies to the Cloud Service concerned, (b) such third party certification or audit provided by the CSP is valid, (c) such third-party certification or audit has assessed and sufficiently reported compliance with the mapped controls of the third-party certification or audit concerned. Provided that the aforementioned criteria are met, the Monitoring Body may consider such third-party certifications or audits as sufficient evidence for the compliance with the Code.

Within Initial Assessments, the Monitoring Body selects an appropriate share of Controls that will undergo in-depth scrutiny, e.g., by sample-taking and request for further, detailed information including potentially confidential information. Within any other Recurring Assessment, the Monitoring Body will select an appropriate share of Controls provided both that over a due period every Control will be subject to scrutiny by the Monitoring Body and aspects of increased attention as indicated e.g., by media reports, publications and actions of supervisory authorities are covered.

If the responses of the CSP satisfy the Monitoring Body, especially if responses are consistent and of appropriate quality and level of detail, reflecting the requirements of the Controls and indications for

appropriate implementation by the Control Guidance, then the Monitoring Body verifies the service(s) declared adhered as compliant and thereupon make them subject to continuous monitoring.

3.4.1 Levels of Compliance

V2.11 of the Code provides three different levels of Compliance. The different levels of compliance relate only to the levels of evidence that are submitted to the Monitoring Body. There is however no difference in terms of which parts of the Code are covered since adherent Cloud Services have to comply with all provisions of the Code and their respective Controls.

3.4.1.1 First Level of Compliance

The CSP has performed an internal review and documented its implemented measures proving compliance with the requirements of the Code with regard to the declared Cloud Service and confirms that the Cloud Service fully complies with the requirements set out in this Code and further specified in the Controls Catalogue. The Monitoring Body verifies that the Cloud Service complies with the Code by information originating from the CSP.

3.4.1.2 Second Level of Compliance

Additional to the "First Level of Compliance", Compliance with the Code is partially supported by independent third-party certificates and audits, which the CSP has undergone with specific relevance to the Cloud Service declared adherent and which were based upon internationally recognised standards procedures. Any such third-party certificates and audits that covered controls similar to this Code, but not less protective, are considered in the verification process of the Monitoring Body. Each third-party certificates and audits that were considered in the verification process by the Monitoring Body shall be referred in the Monitoring Body's report of verification, provided that the findings of such certificates were sufficiently and convincingly reported and documented towards the Monitoring Body and only to the extent such certificates and audits are in line with the Code. The CSP must notify the Monitoring Body if there are any changes to the provided certificates or audits.

The Controls Catalogue may give guidance on third-party certificates and audits that are equivalent to certain Controls in terms providing evidence of complying with the Code.

However, to those Controls that the CSP has not provided any equivalent third-party certificate or audit, the Monitoring Body verifies that the Cloud Service complies with the Code by information originating from the CSP.

The Monitoring Body may refuse application of Second Level of Compliance if third party certificates and audit reports, that are recognized by the Monitoring Body in the verification process concerned,

are not covering an adequate share of Controls of this Code; such adequate share shall be subject to the discretion of the Monitoring Body, considering e.g., the share related to the overall amount of Controls of the Code or whether a full Section or topic is being covered.

3.4.1.3 Third Level of Compliance

Identical to the "Second Level of Compliance" but Compliance is fully supported by independent third-party certificates and audits, which the CSP has undergone with regard to the Cloud Service declared adherent and which were based upon internationally recognized standards.

To the extent a CSP refers to individual reports, such as ISAE-3000 reports, the CSP shall ensure that such reports provide sufficient and assessable information and details on the actual measures implemented by the CSP regarding the Cloud Service concerned. The Monitoring Body shall, if considered necessary, in consultation with the Steering Board, define further requirements on such individual reports, such as accreditation and training for auditors against the provisions and requirements of this Code.

3.4.2 Final decision on the applicable Level of Compliance

When declaring its Cloud Service adherent, the CSP indicates the Level of Compliance it is seeking to achieve. Any final decision, whether a CSP is meeting the requirements of a specific Level of Compliance is up to the sole discretion of the Monitoring Body.

3.5 Transparency about adherence

Each service adherent to the EU Cloud CoC must transparently communicate its adherence by both using the appropriate Compliance Mark[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 Alibaba Cloud (see 2.)

4.1 Fact Finding

Following the declaration of adherence of Alibaba Cloud (Singapore) Private Limited ('**Alibaba Cloud**'), the Monitoring Body provided Alibaba Cloud with a template, requesting Alibaba Cloud to detail its compliance with each of the Controls of the EU Cloud CoC. Additionally, the Monitoring Body requested

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

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.

As this declaration of adherence is a renewal, the Monitoring Body also requested from Alibaba Cloud a comparison of the declared services of last year and this year. It also requested to indicate notably, any services that are no longer included in the declaration of adherence and, where applicable, provide the Monitoring Body with adequate reasons. It shall also be noted, that Alibaba Cloud submitted its renewal according to the deadlines by the Monitoring Body. The renewal process has been prepared by Alibaba Cloud. Delays in the processing of the validation do not indicate any non-compliance of the CSP but were solely related to information gathering and alignment. Given the total amount of Cloud Services subject to this Declaration of Adherence this required more time than originally expected. Consequently, Monitoring Body concludes[14] continuous compliance with the Code.

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 Alibaba Cloud.

Alibaba Cloud declared services have been externally certified and audited, e.g. Alibaba Cloud holds current SOC 2, ISO 27001 and 27017 certificates. The declaration of adherence referred to the respective ISO 27001 audit report 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. Controls were selected for an in-depth assessment based on the several aspects, such as applied changes since the last assessment, ambiguities in responses, current relevant matters from a general data protection point of view, e.g., updated Standard Contractual Clauses (SCC).

[14] See Section 5.
[15] https://eucoc.cloud/en/about/about-eu-cloud-coc/applicable-procedures/

4.3 Examined Controls and related findings by the Monitoring Body

4.3.1 Examined Controls

The Monitoring Body reviewed the initial submission from Alibaba Cloud which outlined how all the requirements of the Code were met by Alibaba Cloud 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.D, 5.1.E, 5.1.G, 5.2.E, 5.2.F, 5.2.G, 5.3.A, 5.3.C-5.3.E, 5.3.G, 5.4.B, 5.4.D, 5.4.E, 5.5.D, 5.5.F, 5.6.A, 5.7.E, 5.7.F, 5.8.A, 5.9.A, 5.9.B, 5.11.B, 5.12.C-5.12.G, 5.13.B, 5.14.C, 5.14.D, 6.1.A, 6.1.C, 6.1.D, 6.2.P.

4.3.2 Findings by the Monitoring Body

During the process of verification Alibaba Cloud consistently shown goodwill. CSP was always available to answer questions from the Monitoring Body, either in writing or via interview. 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 performed an assessment on the applicability of an overarching technical and organizational framework. For this purpose, Monitoring Body was pointed to Alibaba Cloud's Security Whitepaper, which has been updated since the last assessment. Monitoring Body concluded that the Security Whitepaper strongly indicates the overarching framework, alongside detailed information relevant for Customers. Monitoring Body also evaluated suitability of Ding Talk to be considered part of the Cloud Service family and concluded positively.

The Monitoring Body performed an in-depth assessment on the data protection training provided to the personnel processing Customer Personal Data. Alibaba Cloud indicated that all personnel involved in the processing of the Customer Personal Data receive adequate security and data protection trainings as relevant for their role and job function. Alibaba Cloud also clarified that personnel is made aware of applicable procedures and safeguards via regular trainings, which are constantly updated.

Alibaba Cloud also confirmed that its implementation of documented procedures to ensure that its personnel is aware of the adherence to and the requirements of the Code to adequately deal with related Customer inquiries.

Another area of focus related to retention policies. The Code requires that CSPs either communicate and enforce retention policies generally applicable to the Cloud Service or enable the Customer to

manage data retention of Customer Personal Data individually and autonomously. Alibaba Cloud Customers are enabled to manage data retention of Customer Personal Data individually and autonomously. General data retention policies managed by Alibaba Cloud do not apply.

Alibaba Cloud safeguards any third country transfer utilizing SCCs respectively SDPCs at a minimum. Consequently, a distinct documentation per transfer identifying the mechanisms is not considered necessary, neither the monitoring of alternative mechanisms. Additionally, Monitoring Body received confirmation that the updated version of the SCC (SDPC) will be incorporated in accordance with the determined deadlines.

Furthermore, procedures related to Customer's Audit Right were assessed, particularly focussing on the additional evidence of compliance that may be provided by different means other than offered by the Customer Audit Right mechanism. Procedurally, Alibaba Cloud considers any request – including requests for additional (document) evidence of compliance – as a performance of Customer Audit Right, ensuring adequate and timely responses. Based on the information provided, the application of the procedures does not necessarily trigger additional costs for Customers. Consequently, the Monitoring Body concluded Alibaba Cloud has implemented appropriate means to adequately react to Customer requests for additional evidence.

Monitoring Body paid attention to appropriate procedures enabling Alibaba Cloud to respond to authority requests. Alibaba Cloud provided information supporting its capabilities to adequately react on supervisory authorities' requests. Supervisory authorities are expected to reach out by distinct communication channels, which is the privacy contact. Also, in cases where supervisory authorities may not reach out via expected communication channels, Alibaba Cloud implemented safeguard to internally assess, categorize and re-assign the request.

5 Conclusion

Given answers by Alibaba Cloud were consistent. Where necessary Alibaba Cloud 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[16] alongside this report.

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

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

6 Validity

This verification is valid for one year. The full report consists of 14 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[17].

Verification-date: June 2021 **Valid until**: June 2022

Verification-ID: 2020LVL02SCOPE013

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