SCOPE EUROPE

Verification of Declaration of Adherence

Declaring Company: Alibaba Cloud (Singapore) Private Limited

EU CLOUD COC

Verification-ID	2020LVL02SCOPE013
Date of Approval	June 2022
Valid until	June 2023

Table of Contents

1 Verification against v2.11 of the EU Cloud CoC

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

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

2 List of declared services

2.1 Alibaba Cloud products and services

Alibaba Cloud is committed to building a public, open, and secure cloud computing service platform. 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
- Resource Orchestration Service
- E-HPC
- ECS Bare Metal Instance
- Super Computing Cluster
- Function Compute
- Batch Compute
- Dedicated Host
- Operation Orchestration Service
- Elastic Desktop Service
- Compute Nest
- Serverless Application Engine
- Serverless Workflow

[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
- PrivateLink
- Global Accelerator
- Global Traffic Manager
- Secure Content Delivery
- Edge Node Service (ENS)

2.1.3 Database

- ApsaraDB for OceanBase
- ApsaraDB for Redis
- ApsaraDB RDS for MySQL
- ApsaraDB RDS for SQL Server
- ApsaraDB RDS for PostgreSQL
- ApsaraDB for MongoDB
- Data Transmission Service
- AnalyticDB for PostgreSQL
- Time Series Database ("TSDB")
- ApsaraDB for MariaDB TX
- Database Backup
- Data Management
- Data Lake Analytics
- PolarDB
- PolarDB-X
- ApsaraDB for MyBase
- ApsaraDB for HBase
- Database Autonomy Service
- AnalyticDB for MySQL
- ApsaraDB for ClickHouse
- Time Series Database for InfluxDB
- DBStack

2.1.4 Storage

- Tablestore
- Hybrid Cloud Storage
- Data Transport
- Hybrid Backup Recovery
- Cloud Storage Gateway
- Object Storage Service ("OSS")
- Apsara File Storage NAS
- Elastic Block Storage
- Storage Capacity Unit
- Hybrid Cloud Distributed Storage

2.1.5 Security

- Anti-DDoS
- Cloud Firewall
- Web Application Firewall
- SSL Certificates Service

- 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")
- Key Management Service
- Penetration Service
- Fraud Detection

2.1.6 Enterprise Applications & Cloud Communication

- Domains
- Alibaba Cloud DNS
- Dedicated DingTalk
- Short Message Service (SMS)
- Intelligent Robot
- Blockchain as a Service
- API Gateway
- Direct Mail
- Alibaba Mail
- Robotic Process Automation
- YiDA
- GoChina ICP Filing Assistant
- WHOIS
- ZOLOZ Real ID
- ZOLOZ Smart AML
- Alibaba eKYC
- CloudQuotation
- CloudESL
- CloudAP

2.1.7 Analytics

- E-MapReduce
- MaxCompute
- DataWorks
- Data Integration
- Quick BI
- DataV
- Intelligent Robot
- Dataphin
- Elasticsearch
- Realtime Compute for Apache Flink
- Log Service
- Hologres
- Data Lake Formation
- DataHub
- OpenSearch
- AIRec

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 for 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
- Application Configuration Management
- Tracing Analysis
- Application Real-Time Monitoring Service
- Application High Availability Service
- AliwareMQ for IoT
- Message Queue for Apache Kafka
- AlibabaMQ for Apache RocketMQ
- Message Service
- Microservices Engine
- EventBridge
- Message Queue for RabbitMQ

2.1.11 Developer Services

- Cloud Shell
- ActionTrail
- OpenAPI Explorer
- CloudMonitor
- Resource Access Management
- Cloud Config
- Resource Management
- Mobile Testing
- mPaaS

2.1.12 Internet of Things

- IoT Platform
- Link IoT Edge

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].

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

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 in 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 on 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 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

[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/

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 that over a due period every Control will be subject to scrutiny by the Monitoring Body. Where applicable, aspects of current attention at the time of assessment shall be covered, too, e.g., where such aspects were indicated in media reports, publications or actions of supervisory authorities.

If the responses of the CSP satisfy the Monitoring Body, especially if responses are consistent and of appropriate quality and level of detail, reflecting the requirements of the Controls and indications for appropriate implementation by the Control Guidance, then the Monitoring Body verifies the service(s) declared adhered as compliant and thereupon makes them subject to continuous monitoring.

3.4.1 Levels of Compliance

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

3.4.1.1 First Level of Compliance

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

3.4.1.2 Second Level of Compliance

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

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

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

The Monitoring Body may refuse application of Second Level of Compliance if third party certificates and audit reports, that are recognized by the Monitoring Body in the verification process concerned, are not covering an adequate share of Controls of this Code; such adequate share shall be subject to the discretion of the Monitoring Body, considering e.g., the share related to the overall amount of Controls of the Code or whether a full Section or topic is being covered.

3.4.1.3 Third Level of Compliance

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

To the extent a CSP refers to individual reports, such as ISAE-3000 reports, the CSP shall ensure that such reports provide sufficient and assessable information and details on the actual measures implemented by the CSP regarding the Cloud Service concerned. The Monitoring Body shall, if 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.

As this declaration is a renewal[14], the Monitoring Body requested from Alibaba Cloud a confirmation that there has been no material change to the applicable technical and organisational, including contractual, framework. The Monitoring Body also asked from Alibaba Cloud a comparison of the declared serviced of last year and this year and to explicitly indicate any services that are no longer included in the declaration of adherence and, were applicable, provide the Monitoring Body with adequate reasons.

---

[12] https://eucoc.cloud/en/public-register/levels-of-compliance/
[13] https://eucoc.cloud/en/public-register/
[14] You can access the Verification Reports of previous years via the following links: Verification Report 2020, Verification Report 2021

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 Cloud Services subject to this declaration of adherence have been externally certified and audited, e.g., Alibaba Cloud holds current ISO 27K series certificates, C5 and SOC 2 report.

Notwithstanding other certifications, the declaration of adherence referred to 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.

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.A, 5.1.C, 5.1.H, 5.2.A-D, 5.3.D, 5.3.E, 5.3.G, 5.4.E, 5.5.C, 5.5.E, 5.5.F, 5.7.E, 5.7.F, 5.11.B, 5.12.A-C, 5.12.E, 5.12.F, 5.14.A, 5.14.D, 5.14.E, 6.1.A and 6.2.H.

4.3.2 Findings by the Monitoring Body

In light of the Monitoring Body's requests (see section 4.1), Alibaba Cloud indicated that no relevant changes to the Cloud Service Family were applied in regards of the implemented technical and organisational framework. Alibaba Cloud declared additional Cloud Services compared to last year Declaration of Adherence. In that regard, Alibaba Cloud confirmed that the added Cloud Services subject to this year Declaration of Adherence share the same implemented technical and organisational, including contractual framework as the Cloud Services already adherent. In regard to Cloud Services that are no longer in scope of this year's Declaration of Adherence, Alibaba Cloud provided information allowing for such a limitation in compliance with the Code's and Monitoring Body's procedures. The Monitoring Body verified the ISO 27001 certificate's scope with the scope of this Declaration of

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

Adherence. To the minor extent deviations were identified, Alibaba Cloud explained that such deviations result from different verification respectively certification cycles. Alibaba Cloud confirmed, that all Cloud Services within the scope of this Declaration of Adherence are subject to the same implemented measures and that the ISO certificate will be updated accordingly in its next iteration.

The Monitoring Body assessed the constellation of applicable cloud contractual documents and their interrelation. Alibaba Cloud implemented an overarching agreement, i.e., the Cloud Service Agreement. The Cloud Service Agreement is supplemented by specific agreements further aligning with specific needs, e.g., whether or not the primary contracting party is within or outside the EU/EEA. Provided the information and confirmations by Alibaba Cloud regardless of the scenario in question, and therefore, the applicable specific agreements, all the elements put forward by Alibaba Cloud to demonstrate and underpin its compliance with the Code are valid and present in both scenarios.

Regarding the possibility for the Customers to retrieve their Customer Personal Data, Alibaba Cloud makes available, on their website, the necessary information to inform Customers about data formats, export mechanism, technical requirements etc. Additionally, Alibaba Cloud provides product features to assist Customers to download or export the entrusted Personal Data. In total the information provided allowed the Monitoring Body to conclude that Customers have the capability to retrieve their Personal Data promptly and without hindrance.

When it comes to deletion, Alibaba Cloud indicated that the process is immediate.

5 Conclusion

The information provided 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 section 1. The services will be listed in the Public Register of the EU Cloud CoC[16] alongside this report.

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.

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

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 2022 **Valid until**: June 2023

Verification-ID: 2020LVL02SCOPE013

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