SCOPE EUROPE

Verification of Declaration of Adherence

Declaring Company: Alibaba Cloud (Singapore) Private Limited

Verification-ID	2020LVL02SCOPE013
Date of Approval	June 2024
Valid until	June 2025

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

2 List of declared services

2.1 Alibaba Cloud products and services[6]

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.[7]

2.1.1 Elastic Computing

- Elastic Compute Service (ECS)
- Simple Application Server
- Elastic GPU Service
- Auto Scaling
- Resource Orchestration Service
- Elastic High Performance Computing
- ECS Bare Metal Instance
- Function Compute
- Batch Compute
- Dedicated Host
- CloudOps Orchestration Service
- WUYING Worspace
- Compute Nest
- Serverless Application Engine
- CloudFlow
- Alibaba Cloud Linux
- Alibaba Cloud VMware Service
- Edge Network Acceleration

---

[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://www.alibabacloud.com/
[7] **NOTE**: The content for the service description has been provided by the CSP and does not reflect any opinion of or assessment by the Monitoring Body.

- CloudBox

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 Address
- VPN Gateway
- NAT Gateway
- Cloud Enterprise Network (CEN)
- Smart Access Gateway
- Data Transfer Plan
- Alibaba Cloud PrivateZone
- PrivateLink
- Global Accelerator
- Edge Node Service (ENS)
- Network Intelligence Service (NIS)
- Transit router
- Cloud Data Transfer

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
- ApsaraDB for MariaDB
- Database Backup
- Data Management
- PolarDB
- ApsaraDB for MyBase
- ApsaraDB for HBase
- Database Autonomy Service
- AnalyticDB for MySQL
- ApsaraDB for ClickHouse
- Lindorm
- Tair

2.1.4 Storage

- Tablestore
- Data Transport
- Cloud Backup
- Cloud Storage Gateway
- Object Storage Service (OSS)
- Apsara File Storage NAS
- Elastic Block Storage
- Storage Capacity Unit
- Drive and Photo Service

2.1.5 Security

- Anti-DDoS
- Cloud Firewall
- Web Application Firewall
- Certificate Management Service

- Managed Security Service
- Content Moderation
- Security Center
- Bastionhost
- Cloud Hardware Security Module
- Identity as a service (IDaaS)
- Data Security Center
- Key Management Service
- Fraud Detection
- ID Verification

2.1.6 Enterprise Applications & Cloud Communication

- Domain Names
- Alibaba Cloud DNS
- Short Message Service (SMS)
- Blockchain as a Service
- API Gateway
- Direct Mail
- Alibaba Mail
- CloudQuotation
- Chat App Message Service
- Energy Expert
- Voice Service
- Phone Number Verification Service

2.1.7 Analytics

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

2.1.8 Artificial Intelligence

- Image Search
- Platform for AI
- Machine Translation
- Intelligent Speech Interaction
- Vector Retrieval Service
- PAI-Lingjun Intelligent Computing Service

2.1.9 Media Services

- ApsaraVideo Live
- ApsaraVideo for Media Processing
- ApsaraVideo VOD

2.1.10 Container & Middleware

- Enterprise Distributed Application Service
- Managed Service for OpenTelemetry
- Application Real-Time Monitoring Service
- Application High Availability Service
- ApsaraMQ
- ApsaraMQ for Kafka
- Elastic Container Instance
- Container Service for Kubernetes (ACK)
- Container Registry
- Service Mesh
- Message Service
- Microservices Engine
- EventBridge
- Distributed Cloud Container Platform for Kubernetes
- Managed Service for Prometheus
- Managed Service for Grafana

2.1.11 Developer Services

- Resource Access Management
- Cloud Config
- ActionTrail
- OpenAPI Explorer
- Cloud Shell
- CloudMonitor
- EMAS
- mPaaS
- Cloud Architect Design Tools (CADT)
- Cloud Governance Center (CGC)
- Quota Center
- Intelligent Advisor
- Alibaba Cloud DevOps Pipeline
- Cloud Migration Hub

2.1.12 Internet of Things

- IoT Platform
- Alibaba Cloud Link ID²
- 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[8].

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[9].

The Code has been officially approved in May 2021[10]. SCOPE Europe has been officially accredited as Monitoring Body in May 2021[11]. 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.[12]

3.2 Principles of the Verification Process

Notwithstanding the powers of and requirements set out by the supervisory authority pursuant to Article 41 GDPR, the Monitoring Body will assess whether a Cloud Service, that has been declared adherent to the Code, is compliant with the requirements of the Code - especially as laid down in the Controls Catalogue. Unless otherwise provided by the Code, the Monitoring Body's assessment process will be based on an evidence-based conformity assessment, based on interviews and document reviews; proactively performed by the Monitoring Body.

To the extent the Monitoring Body is not satisfied with the evidence provided by a CSP with regards to the Cloud Service to be declared adherent to the Code, the Monitoring Body will request additional information. Where the information provided by the CSP appears to be inconsistent or false, the Monitoring Body will - as necessary - request substantiation by independent reports.

3.3 Multiple Safeguards of Compliance

Compliance of adherent services is safeguarded by the interaction of several mechanisms, i.e., continuous, rigorous, and independent monitoring, an independent complaints' handling process, and

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

finally any CSP declaring services adherent is subject to substantial remedies and penalties in case of any infringement.

3.4 Process in Detail

It is expected that, prior to any assessment of the Monitoring Body, each CSP assesses its compliance internally. When declaring its service(s) adherent to the EU Cloud CoC, each CSP must elaborate its compliance with each of the Controls as provided by the Code considering the Control Guidance, as provided by the Controls Catalogue, to the Monitoring Body.

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

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

Within Initial Assessments, the Monitoring Body selects an appropriate share of Controls that will undergo in-depth scrutiny, e.g., by sample-taking and requesting further, detailed information including potentially confidential information. Within any other Recurring Assessment, the Monitoring Body will select an appropriate share of Controls provided that over a due period every Control will be subject to scrutiny by the Monitoring Body. Where applicable, aspects of current attention at the time of assessment shall be covered too, e.g., where such aspects were indicated in media reports, publications or actions of supervisory authorities.

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

3.4.1 Levels of Compliance

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

3.4.1.1 First Level of Compliance

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

3.4.1.2 Second Level of Compliance

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

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

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

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

3.4.1.3 Third Level of Compliance

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

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

3.4.2 Final decision on the applicable Level of Compliance

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

3.5 Transparency about adherence

Each service adherent to the EU Cloud CoC must transparently communicate its adherence by both using the appropriate Compliance Mark[13] and referring to the Public Register of the EU Cloud CoC[14] 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[15], the Monitoring Body requested from Alibaba Cloud a confirmation that there has been no material change to the applicable technical and organisational and contractual framework. The Monitoring Body also requested from Alibaba Cloud a comparison of the declared

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

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.

Alibaba Cloud 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[16], the Monitoring Body analysed the responses and information provided by Alibaba Cloud.

Alibaba Cloud's declared services have been externally certified and audited. Alibaba Cloud holds a current ISO 27001 certificate, which is valid for the duration of the Declaration of Adherence. Where due to different lifecycles of certifications and adherence, cloud services were not explicitly covered by third-party certifications or attestations, the Monitoring Body concluded that there is no reason to doubt the equivalent implementation for every indicated Cloud Service. Accordingly, Alibaba Cloud confirmed that relevant certifications or attestations will be aligned in respect of their scopes, once possible.

The declaration of adherence referred to the respective ISO 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 verified the certification and references. Further in-depth checks were not performed, as provided third-party certifications adequately indicated compliance.

[16] 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 submission from Alibaba Cloud which outlined how all the requirements of the Code were met by Alibaba Cloud'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.D, 5.3.D, 5.3.E, 5.4.E, 5.5.F, 5.7.E, 5.8.A, 5.10.A, 5.10.B, 5.12.A and 5.13.A.

4.3.2 Findings by the Monitoring Body

During the process of verification, Alibaba Cloud consistently prepared the Declaration of Adherence well and thoroughly. Alibaba Cloud'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), Alibaba Cloud 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, Alibaba Cloud provided explicit confirmation that such Cloud Services belong to the same Cloud Service Family.

Alibaba Cloud provided information indicating that its adherence to the Code is adequately communicated publicly and towards its employees. Consequently, Alibaba Cloud's personnel are enabled to adequately respond to any related Customer inquiries. The information provided to the Monitoring Body indicated that employees and contractors are subject to appropriate confidentiality obligations before engaging in data processing activities.

The Monitoring Body assessed the subprocessor management process. Based on the information provided by Alibaba Cloud, a list of subprocessors with general information is available to the Customer. Moreover, Alibaba Cloud has implemented procedures that ensure a flow down data protection obligations and appropriate technical and organisational measures no less protective than provided by Alibaba Cloud to the Customer.

The Code requires CSPs to assist Customers to respond to Data Subjects' Requests (DSRs). Alibaba Cloud indicated to provide Customers with assistance to deal with DSRs. Additionally, Alibaba Cloud

has a documented procedure to review services and products from a privacy perspective to support Customers with data subject requests.

The assessment involved the procedures ensuring the reporting of data breaches to the Customer. In the event Alibaba Cloud becomes aware of a breach of its security, leading to a personal data breach, Alibaba Cloud has Privacy Incident Response Operating Procedures to notify Customers through appropriate channels without undue delay.

Alibaba Cloud confirmed that Customers have full control over their data management and that Alibaba Cloud only processes data based on the Customer's documented instructions. In the same vein, Alibaba Cloud makes available an up-to-date and accurate Records of Processing Activities (ROPA) for Customers to access independently.

Another area of the assessment has been third country transfers. Alibaba Cloud indicated that it relies on the appropriate data transfer safeguards as provided by Chapter V GDPR. The Monitoring Body received information confirming that Alibaba Cloud relies on adequacy decisions and – overarchingly – that Standard Contractual Clauses (SCCs) are in place. In this context, Alibaba Cloud assesses and monitors whether a country that is the destination of a data transfer is subject to an adequacy decision of the European Commission.

Furthermore, the Monitoring Body has assessed Customer's Audit Rights. Alibaba Cloud makes publicly available independent third-party audit reports and certifications, and Customers can request additional evidence or assistance via the trust center. Alibaba Cloud indicated that Customers are not charged for performing their Audit Rights. If third-party auditors are appointed by Customers, Customers will have to bear related costs.

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 1. The service(s) will be listed in the Public Register of the EU Cloud CoC[17] alongside this report.

[17] 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[18].

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

Verification-ID: 2020LVL02SCOPE013

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