

Verification of Declaration of Adherence

Declaring Company: Alibaba Cloud (Singapore) Private Limited



EU
CLOUD
COC

Verification-ID 2020LVL02SCOPE013

Date of Approval June 2026

Valid until June 2027

Table of Contents

1	Verification against v2.11 of the EU Cloud CoC	4
2	List of declared services	4
2.1	Alibaba Cloud	4
2.1.1	Computing	4
2.1.2	Networking & CDN	5
2.1.3	Database	5
2.1.4	Storage	5
2.1.5	Security	5
2.1.6	Enterprise Services & Cloud Communication	6
2.1.7	Analytics Computing	6
2.1.8	AI & Machine Learning	6
2.1.9	Media Services	6
2.1.10	Middleware	7
2.1.11	Container	7
2.1.12	Developer Tools	7
2.1.13	Domain Names and Websites	7
2.1.14	Serverless	7
2.1.15	Migration & O&M Management	7
3	Verification Process - Background	8
3.1	Approval of the Code and Accreditation of the Monitoring Body	8
3.2	Principles of the Verification Process	8
3.3	Multiple Safeguards of Compliance	8
3.4	Process in Detail	9
3.4.1	Levels of Compliance	10

3.4.2	Final decision on the applicable Level of Compliance	11
3.5	Transparency about adherence	11
4	Assessment of declared services by Alibaba (see 2.)	11
4.1	Fact Finding	11
4.2	Selection of Controls for in-depth assessment	12
4.3	Examined Controls and related findings by the Monitoring Body	12
4.3.1	Examined Controls	12
4.3.2	Findings by the Monitoring Body	13
5	Conclusion	14
6	Validity	14

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' or 'Code'**)¹ in its version 2.11 (**'v2.11'**)² as of December 2020.

Originally drafted by the Cloud Select Industry Group³ (**'C-SIG'**) the EU Cloud CoC – at that time called C-SIG Code of Conduct on data protection for Cloud Service Providers (**'CSPs'**) – was developed against Directive 95/46/EC⁴ 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 Cloud⁶

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 Computing

- Elastic Compute Service (ECS)
- Simple Application Server (SAS)
- Elastic GPU Service
- Auto Scaling
- Elastic High Performance Computing (E-HPC)
- ECS Bare Metal Instance
- Function Compute (FC)
- Dedicated Host
- Elastic Desktop Service (EDS)
- Compute Nest
- Serverless App Engine (SAE)
- Alibaba Cloud Linux
- Edge Network Acceleration (ENA)
- CloudBox
- Cloud Phone
- Edge Node Service (ENS)
- Elastic Container Instance (ECI)

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.

- App Streaming

2.1.2 Networking & CDN

- CDN
- Edge Security Acceleration (ESA)
- Server Load Balancer (SLB)
- Virtual Private Cloud (VPC)
- Express Connect
- Elastic IP Address (EIP)
- VPN Gateway (VPN)
- NAT Gateway
- Cloud Enterprise Network (CEN)
- Smart Access Gateway (SAG)
- Data Transfer Plan
- Alibaba Cloud DNS PrivateZone
- PrivateLink
- Global Accelerator (GA)
- Network Intelligence Service (NIS)
- Transit Router (TR)
- Cloud Data Transfer (CDT)

2.1.3 Database

- ApsaraDB RDS
- ApsaraDB for MongoDB
- Data Transmission Service
- AnalyticDB
- Data Management (DMS)
- PolarDB
- ApsaraDB for HBase
- Database Autonomy Service (DAS)
- ApsaraDB for ClickHouse
- Lindorm
- Tair (Redis OSS-Compatible)
- ApsaraDB for SelectDB

2.1.4 Storage

- Tablestore
- Data Transport
- Cloud Backup
- Cloud Storage Gateway (CSG)
- Object Storage Service (OSS)
- File Storage NAS
- Elastic Block Storage (EBS)
- Storage Capacity Unit (SCU)
- Drive and Photo Service
- Intelligent Media Management
- Simple Log Service (SLS)
- Cloud Parallel File Storage (CPFS)
- Backup and Disaster Recovery Center (BDRC)

2.1.5 Security

- Anti-DDoS
- Cloud Firewall
- Web Application Firewall (WAF)
- Certificate Management Service (Original SSL Certificate)
- Managed Security Service (MSS)
- AI Guardrails
- Security Center
- Bastion Host
- Cloud Hardware Security Module (HSM)

- Identity as a Service (IDaaS)
- Data Security Center (Original SDDP)
- Key Management Service (KMS)
- Fraud Detection
- ID Verification
- Secure Access Service Edge (SASE)
- Resource Access Management (RAM)
- Captcha

2.1.6 Enterprise Services & Cloud Communication

- Short Message Service (SMS)
- Blockchain as a Service (BaaS)
- Direct Mail
- Alibaba Mail
- CloudQuotation
- Chat App Message Service
- Energy Expert
- Voice Service (VS)
- Phone Number Verification Service

2.1.7 Analytics Computing

- E-MapReduce
- MaxCompute
- DataWorks
- Data Integration
- Quick BI
- DataV
- Elasticsearch
- Realtime Compute for Apache Flink
- Hologres
- Data Lake Formation (DLF)
- DataHub
- Dataphin
- Quick Audience
- Quick Tracking
- Vector Retrieval Service for Milvus

2.1.8 AI & Machine Learning

- OpenSearch
- AIRec
- Image Search
- Platform for AI (PAI)
- Machine Translation
- Intelligent Speech Interaction
- Intelligent Computing Service PAI-Lingjun
- Alibaba Cloud Model Studio
- Chatbot
- DashVector

2.1.9 Media Services

- ApsaraVideo Live
- ApsaraVideo Media Processing (MPS)
- ApsaraVideo VOD
- ApsaraVideo Real-time Communication
- Intelligent Media Services (IMS)

2.1.10 Middleware

- API Gateway
- Enterprise Distributed Application Service (EDAS)
- Managed Service for OpenTelemetry
- Application Real-Time Monitoring Service (ARMS)
- Application High Availability Service (AHAS)
- ApsaraMQ
- ApsaraMQ for Kafka
- Simple Message Queue (formerly MNS)
- Microservices Engine (MSE)
- EventBridge
- Managed Service for Prometheus
- Managed Service for Grafana

2.1.11 Container

- Container Service for Kubernetes (ACK)
- Container Registry (ACR)
- Service Mesh (ASM)
- Container Compute Service (ACS)
- Distributed Cloud Container Platform for Kubernetes

2.1.12 Developer Tools

- Resource Orchestration Service (ROS)
- OpenAPI Explorer
- Cloud Shell
- HTTPDNS
- mPaaS
- Alibaba Cloud DevOps
- AI Coding Assistant Lingma

2.1.13 Domain Names and Websites

- Alibaba Cloud DNS (DNS)
- Domain Names and Website

2.1.14 Serverless

- CloudFlow

2.1.15 Migration & O&M Management

- CloudOps Orchestration Service
- CloudConfig
- ActionTrail
- Cloud Monitor
- Cloud Architect Design Tools (CADT)
- Cloud Governance Center (CGC)
- Quota Center
- Intelligent Advisor
- Cloud Migration Hub (CMH)
- Resource Management

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 GDPR⁸.

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 SRL⁹.

The Code has been officially approved in May 2021¹⁰. SCOPE Europe has been officially accredited as Monitoring Body in May 2021¹¹. 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://euococ.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 Mark¹³ and referring to the Public Register of the EU Cloud CoC¹⁴ to enable Customers to verify the validity of adherence.

4 Assessment of declared services by Alibaba (see 2.)

4.1 Fact Finding

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

As this declaration is a renewal¹⁵, the Monitoring Body requested from Alibaba 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 a comparison of the declared Cloud

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 previous year via the following link: [Alibaba - Verification Report – \(Year\)](#)

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 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 CoC¹⁶, the Monitoring Body analysed the responses and information provided by Alibaba.

Alibaba's declared services have been externally certified and audited. Alibaba holds a 27001 ISO certificate, which is valid for the duration of the Declaration of Adherence, and the scope of registration includes all the declared services. The declaration of adherence referred to the respective ISO 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.

4.3 Examined Controls and related findings by the Monitoring Body

4.3.1 Examined Controls

The Monitoring Body reviewed the submission from Alibaba which outlined how all the requirements of the Code were met by Alibaba's implemented measures. In line with the Monitoring Body's process outlined in Section 3.4, the Monitoring Body selected a subset of Controls from the Code for in-depth scrutiny. In-depth scrutiny reflects sample taking and follow-up questions, whilst the latter may address requests for clarifications or more detailed information. The Controls selected for this level of review were: 5.1.A, 5.1.D, 5.1.E, 5.1.F, 5.1.G, 5.1.H, 5.2.A, 5.3.B, 5.3.C, 5.3.D, 5.3.E, 5.4.A, 5.4.D,

¹⁶ <https://euoc.cloud/en/about/about-eu-cloud-coc/applicable-procedures/>

5.4.E, 5.5.A, 5.5.C, 5.5.F, 5.7.A, 5.7.D, 5.7.F, 5.8.B, 5.9.B, 5.11.A, 5.11.C, 5.12.A, 5.12.C, 5.12.D, 5.13.A, 5.13.B, 5.14.F, 6.1.C, 6.2.H and 6.2.P.

4.3.2 Findings by the Monitoring Body

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

Alibaba has confirmed that a Cloud Services Agreement ("CSA") is in place incorporating, at a minimum, the data protection obligations under the GDPR, no less protective than those set out in the Code. The CSA determines the terms under which the CSP can engage subprocessors, the terms under which the Customer Personal Data shall be processed, and the processing activities in relation to such data engaged in by the CSP and any subprocessors.

Alibaba indicated that its adherence to the Code is communicated to its personnel and that the latter is aware of the adherence to the Code in order to adequately handle related Customer inquiries. Specific policies have been put in place by Alibaba to ensure its personnel is trained appropriately in this regard. In this regard, Alibaba also publicly communicates its adherence to the Code on its website.

The assessment involved the subprocessor management process. Based on the information provided by Alibaba, a process is in place to ensure that the CSP only engages subprocessors that can provide sufficient guarantees of compliance with the GDPR. This procedure considers different elements necessary for the assessment of subprocessors, such as privacy compliance maturity, data processing legal basis, security capability, and data transfer compliance mechanisms. Alibaba has implemented procedures to ensure a flow down of data protection obligations, and that appropriate technical and organisational measures no less protective than the ones provided by the CSP to the Customer are implemented by subprocessors. Moreover, the CSP confirmed that a list of subprocessors with general information on the existing subprocessors and applicable jurisdictions is made available to the Customer through the Data Processing Addendum ("DPA").

When it comes to data breaches, Alibaba provided information on its data breach handling procedure, which is designed to identify, handle and respond to data breaches, should any occur. Alibaba explained the key aspects of these processes to the Monitoring Body. The reporting of the data breaches to Customers is a contractual obligation and such obligation is operationalised through relevant policies and procedures.

Moreover, Alibaba confirmed that all employees and contractors are subject to appropriate confidentiality obligations before being engaged in data processing activities, which continue after the end of the employment or termination of the respective agreements. Training is provided to ensure that personnel involved in the processing of Customer Personal Data are aware of their confidentiality obligations.

In the context of third country transfers, Alibaba indicated that it relies on the appropriate data transfer safeguards as provided by Chapter V GDPR. The Monitoring Body received information from the CSP confirming that Alibaba relies on Adequacy Decisions and Standard Contractual Clauses (“SCCs”), of which the latter applies overarchingly. In addition, Alibaba confirmed that its international compliance team monitors the applicability of existing adequacy decisions.

5 Conclusion

The information provided by Alibaba was consistent. Where necessary, Alibaba 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 CoC¹⁷ alongside this report.

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

6 Validity

This verification is valid for one year. The full report consists of 15 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

¹⁷ <https://euoc.cloud/en/public-register/>

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 CoC¹⁸.

Verification-date: June 2026

Valid until: June 2027

Verification-ID: 2020LVL02SCOPE013

¹⁸ <https://eucoc.cloud/en/public-register/>