SCOPE EUROPE

Verification of Declaration of Adherence

Declaring Company: Sparkoo Technologies Ireland Co., Limited

Verification-ID	2024LVL02SCOPE5418
Date of Approval	March 2024
Valid until	March 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 Huawei Cloud[6]

Sparkoo, as a subsidiary of Huawei Cloud, is in charge of the cloud business for customers in Europe. Sparkoo aims to work together with customers, suppliers, and partners to inspire innovation across industries for a robust ecosystem in an intelligent world, and will continuously make every effort in existing and future collaborations in respect of cloud services and solutions.

Huawei Cloud[7] opens up Huawei's technology achievements and expertise in ICT over three decades into reliable, secure, and sustainable cloud services for customers, partners, and developers. Huawei Cloud provides Everything as a Service, aiming at helping customers unleash the power of digital technology with comprehensive Infrastructure-as-a-Service, Technology-as-a-Service, and Expertise-as-a-Service offerings. Huawei Cloud is committed to building a ubiquitous cloud foundation for an intelligent world. [8]

Everything as a Service: Building the Cloud Foundation for an Intelligent World

- Infrastructure as a Service for global accessibility
- Technology as a Service for easy innovation

---

[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.huaweicloud.com/eu
[7] **NOTE**: The Monitoring Body assessed the Cloud Services dedicated for the European market as provided by Sparkoo.
[8] **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.

- Expertise as a Service for shared excellence

.

2.1.1 Compute

- Elastic Cloud Server (ECS)
- Bare Metal Server (BMS)
- Auto Scaling (AS)
- Image Management Service (IMS)
- FunctionGraph

2.1.2 Containers

- Cloud Container Engine (CCE)
- SoftWare Repository for Container (SWR)

2.1.3 Storage

- Object Storage Service (OBS)
- Elastic Volume Service (EVS)
- Scalable File Service (SFS)
- Cloud Backup and Recovery (CBR)

2.1.4 Networking

- Virtual Private Cloud (VPC)
- Elastic Load Balance (ELB)
- NAT Gateway (NAT)
- Elastic IP (EIP)
- Direct Connect
- Virtual Private Network (VPN)
- VPC Endpoint (VPCEP)
- Cloud Connect (CC)
- Enterprise Router (ER)

2.1.5 Databases

- RDS for MySQL
- RDS for PostgreSQL
- Document Database Service (DDS)
- GaussDB (for MySQL)
- Distributed Database Middleware (DDM)
- Data Replication Service (DRS)
- GeminiDB
- GaussDB
- RDS for SQLServer
- Data Admin Service (DAS)

2.1.6 Artificial Intelligence

- ModelArts
- Graph Engine Service (GES)

2.1.7 Analytics

- Data Lake Insight (DLI)
- Data Warehouse Service (DWS)
- MapReduce Service (MRS)
- DataArts Studio
- Cloud Search Service (CSS)

2.1.8 Middleware

- Distributed Cache Service (DCS) for Redis
- API Gateway (APIG)
- EventGrid (EG)
- Distributed Message Service (DMS) for Kafka
- Distributed Message Service (DMS) for RocketMQ
- Distributed Message Service (DMS) for RabbitMQ

2.1.9 Business Applications

- Domain Name Service (DNS)
- Message & SMS

2.1.10 Security and Compliance

- Anti-DDoS Service (AAD)
- Web Application Firewall (WAF)
- Host Security Service (HSS)
- Data Encryption Workshop (DEW)
- Database Security Service (DBSS)
- Cloud Firewall (CFW)
- Cloud Bastion Host (CBH)
- Data Security Center (DSC)
- Cloud Certificate Manager (CCM)
- Dedicated HSM
- SecMaster

2.1.11 Management and Governance

- Application Operations Management (AOM)
- Cloud Eye
- Identity and Access Management (IAM)
- Cloud Trace Service (CTS)
- Log Tank Service (LTS)
- Simple Message Notification (SMN)
- KooCLI
- Resource Formation Service (RFS)

2.1.12 Migration

- Cloud Data Migration (CDM)

2.1.13 Content Delivery Network and Edge Computing

- Content Delivery Network (CDN)

2.1.14 Media Services

- Live
- Video on Demand (VOD)
- Media Processing Center (MPC)

2.1.15 Internet of Things

- IoT Device Access (IoTDA)

2.1.16 DevOps

- API Explorer

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[9].

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[10].

The Code has been officially approved in May 2021[11]. SCOPE Europe has been officially accredited as Monitoring Body in May 2021[12]. The robust and complex procedures and mechanisms can be

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

reviewed by any third-party in detail at the website of the EU Cloud CoC alongside a short summary thereof.[13]

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 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.

[13] https://eucoc.cloud/en/public-register/assessment-procedure/

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[14] and referring to the Public Register of the EU Cloud CoC[15] to enable Customers to verify the validity of adherence.

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

4.1 Fact Finding

Following the declaration of adherence of Sparkoo Technologies Ireland Co., Limited ('**Sparkoo**'), the Monitoring Body provided Sparkoo with a template, requesting Sparkoo to detail its compliance with each of the Controls of the EU Cloud CoC.

Additionally, the Monitoring Body requested an overview and reasoned response on the actual structure of the services declared adherent and why declared services are to be considered a "service family". A service family requires that all services rely on the same core infrastructure, with regard to hardware and software (i.e., technical framework), and are embedded in the same organisational and contractual framework.

Sparkoo 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. Sparkoo provided information illustrating the actual structure of the services declared adherent and describing the technical, organisational and contractual framework.

4.2 Selection of Controls for in-depth assessment

Following the provisions of the Code and the Assessment Procedure applicable to the EU Cloud CoC[16], the Monitoring Body analysed the responses and information provided by Sparkoo.

---

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

Sparkoo's declared services have been externally certified and audited. Sparkoo holds an 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 Sparkoo which outlined how all the requirements of the Code were met by Sparkoo'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.C, 5.1.D, 5.1.H, 5.2.A-5.2.G, 5.3.C-5.3.F, 5.4.A-5.4.B, 5.4.D-5.4.F, 5.5.A-5.5.F, 5.7.A-5.7.F, 5.8.A-5.8.B, 5.9.A, 5.10.A-5.10.B, 5.11.A-5.11.C, 5.12.A-5.12.G, 5.13.A-5.13.B, 5.14.A-5.14.D, 5.14.F, 6.1.A-6.1.C, 6.2.H, 6.2.I and 6.2.P.

4.3.2 Findings by the Monitoring Body

Monitoring Body verified that declared Cloud Services qualify both as Cloud Service under the Code and as Cloud Service Family. Related to the Monitoring Body's requests (see section 4.1), Sparkoo provided information outlining the structure of the services, contractual and supporting documents enabling the Monitoring Body to better understand Sparkoo's service offerings. Sparkoo provided explicit confirmation that all Cloud Services declared adherent belong to the same Cloud Service Family.

A first area of focus was around engagement of subprocessors. In addition to filling in a due diligence checklist prior to appointing subprocessors and signing Data Processing Agreements with them, Sparkoo has put in place a procedure to ensure that subprocessors engaged provide sufficient guarantees of compliance with the General Data Protection Regulation ('GDPR') throughout the life of the agreement with Sparkoo. Annual risk assessments are also performed by Sparkoo globally for certain types of subprocessors to ensure mitigation of associated risks. Sparkoo has a defined mechanism to notify Customers of the changes in subprocessors. The timelines for objection, as well as the means to do so were confirmed by Sparkoo's contractual documents.

Another focus has been the enablement of Customers, with respect to Customers accessing all relevant information, deletion of Customer Personal Data, as well as responding to Data Subjects Requests. Customers are provided with the possibility to do so through self-service functionalities. Sparkoo confirmed that where Customers may need more information not covered by the self-service functionalities provided, Customers may send requests to Sparkoo via dedicated communication channels to enable the latter to support and assist Customers. Documented procedures provided details on how these requests will be escalated internally to ensure appropriate handling.

Sparkoo's records of processing activities ('ROPA') built another area of focus. Based on the information provided, Sparkoo maintains a ROPA in its capacity as Data Processor, which includes the relevant information as per Article 30.2 GDPR. A dedicated communication channel is available for Customers to reach out to Sparkoo to update the information in the ROPA. The relevant team is automatically notified of such requests and handles them accordingly.

The Monitoring Body also assessed Customers' Audit Rights. Sparkoo sends third-party reports and certification to its Customers, upon their requests and subject to them signing confidentiality agreements. Customers' Audit Rights are a standard part of Sparkoo's Data Processing Addendum ('DPA'). Internal processes have been developed to ensure guidance is provided to relevant departments in assisting with Customers' requested Audits, and includes the process details as well as how related potential security risks are mitigated. Sparkoo's principles in regards of costs determination and allocation related to Customers' Audit Rights were also presented to the Monitoring Body.

Sparkoo confirmed that the infrastructure on which it runs its Cloud Services is in the EU/EEA and Customer Personal Data is not transferred outside the EU/EEA unless specifically requested to do so by the Customer and only on the basis of appropriate safeguards as set out in the GDPR. In case of such third country transfers, Sparkoo has implemented safeguards as provided by Chapter V GDPR, as confirmed by its contractual documents. Standard Contractual Clauses (SCCs) have been implemented as an overarching mechanism for the transfer of Customer Personal Data in Sparkoo's DPA.

Finally, Sparkoo imposes a duty of confidentiality on its employees and contractors alike, which continue after the end of the respective agreements. In the same vein, Sparkoo ensures annual general privacy and security trainings for all its employees, after which an exam must be taken.

5 Conclusion

The information provided by Sparkoo were consistent. Where necessary, Sparkoo 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.

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

6 Validity

This verification is valid for one year. The full report consists of 13 pages in total, whereof this is the last page closing with the Verification-ID. Please refer to the table of contents at the top of this report to verify that the copy you are reading is complete, if you have not received the copy of this report via the Public Register of the EU Cloud CoC[18].

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

Verification-ID: 2024LVL02SCOPE5418

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