Verification of Declaration of Adherence

Declaring Company: EQS Group GmbH

Verification-ID	2025LVL02SCOPE5429
Date of Approval	August 2025
Valid until	August 2026

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' or 'Code'**)[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 (**'CSPs'**) – 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 EQS Compliance COCKPIT[6]

The EQS Compliance COCKPIT is a platform that helps organizations manage compliance, risk, and integrity processes through modular services like whistleblowing, third-party management, policies approvals, and risk tracking. These modules are built on a shared technical infrastructure and contractual framework, ensuring consistent security data management, and service standards.

The platform is either hosted on public (AWS in the EU) or private clouds (Germany, France, Switzerland), including data centers, servers and networks, depending on the customers choice.

The platform consists of independent but interconnected modules (i.e. Integrity Line, Policies, Third Parties, Approvals, Risks) which have their own data and workflows, yet shares the underlying infrastructure, security and user management.

Third-party providers support hosting and network infrastructure, while the software layers are maintained by EQS Group, ensuring flexibility within a cohesive environment.[7]

---

[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.eqs.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.

In scope of the Assessment has been EQS Group Cloud Services including:

- EQS Integrity Line
- EQS Third Parties
- EQS Policies
- EQS Approvals
- EQS Risks

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 SRL[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

[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/

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.

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.

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

4 Assessment of declared services by EQS Group (see 2.)

4.1 Fact Finding

Following the declaration of adherence of EQS Group GmbH ('**EQS Group**'), the Monitoring Body provided EQS Group with a template, requesting EQS Group 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.

EQS Group 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. EQS Group 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[15], the Monitoring Body analysed the responses and information provided by EQS Group.

EQS Group's declared services have been externally certified and audited. EQS Group holds an ISO 27001 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.

[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 submission from EQS Group which outlined how all the requirements of the Code were met by EQS Group'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-C, 5.1.F, 5.2.C, 5.3.C, 5.3.E, 5.4.A, 5.5.A, 5.5.C-E, 5.7.A-B, 5.7.E, 5.8.A, 5.11.B-C, 5.12.D, 5.13.A, 5.14.B, 5.14.E, 5.14.F and 6.1.C.

4.3.2 Findings by the Monitoring Body

During the process of verification, EQS Group consistently prepared the Declaration of Adherence well and thoroughly. EQS Group'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.

The 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), EQS Group provided information outlining the structure of the services, contractual and supporting documents enabling the Monitoring Body to better understand EQS Group's service offerings. EQS Group provided explicit confirmation that all Cloud Services declared adherent belong to the same Cloud Service Family.

The Monitoring Body has focused on the information provided to the Customers. EQS Group indicated that a Cloud Service Agreement ('CSA') is in place with the Customers, incorporating the data protection obligations under GDPR as a minimum and ensuring that they are no less protective than those provided by the Code. The CSA defines the responsibilities of the Customers and the CSP regarding security measures and the terms under which the Customer Personal Data shall be processed. The CSP confirmed that relevant procedures are implemented to safeguard that only subprocessros with sufficient guarantees of compliance with the GDPR are engaged.

The assistance provided to the Customers was assessed by the Monitoring Body. EQS Group confirmed that Customers are provided with various self-service functionalities to deal with the data subject requests ('DSRs') on their own. Such functionalities include, as an example, deletion and retrieval of Customer Personal Data. Further, EQS Group specified that Customers are provided with relevant assistance in conducting their Data Protection Impact Assessment ('DPIA'). Additional support with

DSRs and DPIAs can be requested through a dedicated communication channel. As per established procedures demonstrated by EQS Group, it is ensured that the information provided to Customers in support of their DPIA does not create a security risk for the CSP.

The procedures to deal with supervisory authority requests were also assessed. Requests by supervisory authorities relating to Customer Personal Data were confirmed to be communicated to the Customers, as provided by the Code, with this obligation being reflected in the contractual documents. EQS Group affirmed that appropriate procedures are in place to ensure that responses to requests from supervisory authorities take place in due time and appropriate detail and quality.

Another area of focus was built around Customers' audit rights. In accordance with the information provided, EQS Group makes available the most recent compliance information, including third-party audit reports and certifications, through a dedicated self-service portal upon request. Customers may reach out for support via a dedicated communication channel and get access to the required information via self-service portal. Additionally, EQS Group demonstrated that internal policies and procedures are in place to ensure the provision of compliance information and the enablement of Customer's audit rights, including inspections. EQS Group confirmed that Customer audit costs are not prohibitive or excessive and are mutually agreed upon with Customers.

Records of processing activities (ROPA) have also been a part of the assessment. EQS Group indicated that it maintains an up-to-date and accurate ROPA, including the relevant information as per Article 30.2 GDPR, in its capacity as a Processor. Customers are enabled to provide and update the information relating to the completeness and accuracy of the ROPA via a dedicated communication channel.

Finally, media disposal and data wiping procedures have been part of the assessment. EQS Group confirmed the implementation of relevant policies and procedures to ensure that all storage media used to store Customer Personal Data are securely overwritten or sanitised before those media are re-used or sent for disposal.

5 Conclusion

The information provided by EQS Group were consistent. Where necessary, EQS Group 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[16] alongside this report.

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

6 Validity

This verification is valid for one year. The full report consists of 11 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: August 2025 **Valid until**: August 2026

Verification-ID: 2025LVL02SCOPE5429

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