Verification of Declaration of Adherence

Declaring Company: IBM Corporation

EU CLOUD COC

Verification-ID	2023LVL02SCOPE5316
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 IBM Cloud for Financial Services[6]

IBM Cloud for Financial Services is a public cloud ecosystem developed with and for the financial services industry. It is designed to enable financial institutions to securely host applications and workloads in the public cloud by enabling them to establish their own private cloud-like computing environment on shared public cloud infrastructure that is logically isolated from all other cloud tenants. It includes built-in security and controls capabilities designed to enable clients to automate and monitor their security and compliance controls posture, mitigate cloud risk and accelerate cloud adoption.

IBM Cloud for FS operates on the IBM Cloud Framework for Financial Services, which has been designed to help address the needs of financial services institutions with regulatory compliance, security, and resiliency during the initial deployment phase and with ongoing operations. The framework includes a comprehensive set of controls designed to help address the security requirements and regulatory compliance obligations of financial institutions and cloud best practices and reference architectures designed to facilitate compliance with the control requirements.[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://cloud.ibm.com/docs/framework-financial-services?topic=framework-financial-services-about
[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.

2.1.1 IBM Cloud Virtual Server for VPC

- IBM Dedicated Host for VPC

2.1.2 IBM Cloud Bare Metal Server for VPC

2.1.3 IBM Cloud Flow Logs for VPC

2.1.4 IBM Cloud Virtual Private Cloud

- Load Balancer for VPC
- VPN for VPC: Site-to-site gateway
- VPN for VPC: Client-to-site gateway

2.1.5 IBM Cloud Storage for VPC

- IBM Cloud Block Storage for Virtual Private Cloud
- IBM Cloud Block Storage Snapshots for VPC

2.1.6 IBM Cloud Object Storage

2.1.7 IBM Key Protect for IBM Cloud

2.1.8 IBM Cloud Secrets Manager

2.1.9 IBM Cloud Satellite

2.1.10 IBM Red Hat OpenShift on IBM Cloud

2.1.11 IBM Cloud for VMware Solutions

2.1.12 IBM Cloud Schematics

2.1.13 Hyper Protect Crypto Services

2.1.14 IBM Container Registry

2.1.15 IBM Cloud Continuous Delivery

2.1.16 IBM Code Engine

2.1.17 IBM Cloud Event Notifications

2.1.18 IBM Event Streams for IBM Cloud

2.1.19 IBM Cloud Security and Compliance Center

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]

[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/

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.

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 IBM (see 2.)

4.1 Fact Finding

Following the declaration of adherence of IBM Corporation ('**IBM**'), the Monitoring Body provided IBM with a template, requesting IBM 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 IBM a confirmation that there has been no material change to the applicable technical and organisational and contractual framework. The Monitoring Body also requested from IBM a comparison of the declared 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.

IBM 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.

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

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 IBM.

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

4.3.2 Findings by the Monitoring Body

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

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

The Monitoring has focused on the information provided to the Customers. IBM has indicated that a Cloud Service Agreement is in place with Customers determining: the responsibilities of the Customers and CSP regarding the security measures, terms under which the Customer Personal Data shall be processed, and the scope of Customer's instructions. Additionally, as confirmed by IBM, relevant policies and procedures are in place ensuring that Customer Personal Data is not processed by any personnel for any purpose independent of the instructions of the Customer.

Further, IBM has affirmed that its adherence to the Code is transparently communicated to the Customers and internal policies and procedures are implemented to communicate it to its personnel, ensuring the awareness of the Code requirements and appropriate enablement to deal with related Customer inquiries.

Moreover, Customers have access to dedicated communication channels to request support and access product documentation, including information on the Technical and Organizational measures, compliance information, as well as data formats, processes, technical requirements and timeframes of retrieving the entrusted Customer Personal Data.

When it comes to assistance provided to the Customers, as per the information provided by IBM, Customers are provided with various self-service capabilities allowing them to deal with data subject requests (DSRs) covering: the deletion of Customer Personal Data, and retrieval and export of Customer Personal Data in machine readable, commonly used, structured format.

Additionally, IBM has implemented policies and procedures to provide Customers with assistance to respond to requests by supervisory authorities, including notification of Customers when it receives a request from the supervisory authority pertaining to Customer Personal Data, as provided by the Code. Customers are enabled to reach out for further assistance to IBM, if required.

Data breach notification and reporting obligations have been in the scope of the assessment. In this vein, IBM has identified that the global security and incident management policies and procedures are implemented to identify and handle data breaches, if any such breach may happen. The reporting of the data breaches and Customer notification are part of the relevant policies and procedures and are included in the contractual documentation with the Customers.

In respect of third country transfers. IBM has confirmed that it relies on the relevant data transfer safeguards as provided by Chapter V GDPR such as adequacy decisions and Standard Contractual

Clauses ('SCCs'). SCCs have been indicated to be relied upon as an overarching data transfer safeguard, while the applicability of existing adequacy decisions and applicable legal and regulatory landscape is monitored by a dedicated team, globally.

When it comes to Customer Audit Rights, IBM has provided information that most recent third-party audit reports and certifications are provided to Customers upon request and further information may be requested, if required. Additionally, IBM indicated that it contributes and allows for Customer-requested audits, including on-site inspections, and communicates the relevant procedures to the Customers via the Cloud Service Agreement. The assistance provided by IBM with regards to the performance of Customer's Audit Rights, including on-site inspections, may be subject to additional charges. In this regard, IBM has confirmed to have in place a due methodology to calculate the associated costs, ensuring that such costs are not prohibitive or excessive.

To the extent the subprocessor management program is concerned, IBM provided information that subprocessors are engaged based on the general written authorization and only to the extent it is ensured, that subprocessors provide sufficient guarantees of compliance with the GDPR no less protective as provided by IBM. General information on the subprocessors is communicated to Customers via relevant contractual documentation and is accessible in a dedicated list of subprocessors.

Encryption capabilities of Customer Personal Data have been assessed. It has been provided by IBM that Customer Personal Data is encrypted both while in transit over the public networks and at rest. The state-of-art implementation is maintained by ensuring that relevant personnel will be properly trained and monitors recent development of good practices.

5 Conclusion

The information provided by IBM were consistent. Where necessary, IBM 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 IBM to support the compliance of its service, the Monitoring Body grants IBM 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: June 2024 **Valid until**: June 2025

Verification-ID: 2023LVL02SCOPE5316

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