SCOPE EUROPE

Verification of Declaration of Adherence

Declaring Company: Microsoft Corporation

Verification-ID	2021LVL02SCOPE116
Date of Approval	May 2021
Valid until	May 2022

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 being drafted by the Cloud Select Industry Group[3] (**'C-SIG'**) the EU Cloud CoC, at that time being called C-SIG Code of Conduct on data protection for Cloud Service Providers, the Code was developed against Directive 95/46/EC[4] incorporates 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 Microsoft Azure[6]

Microsoft Azure is a cloud computing platform for building, deploying and managing cloud services through a global network of Microsoft and third-party managed datacenters. It supports both Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) cloud service models, offers more than 200 services, and enables hybrid solutions that integrate cloud services across multiple clouds, on-premises, and at the edge. Azure supports many customers, partners, and government organizations that span across a broad range of products and services, geographies, and industries. Microsoft Azure is designed to meet their security, confidentiality, and compliance requirements.[7] As comprising of:

2.1.1 Compute

App Service
- API Apps
- Mobile Apps
- Web Apps
- Static Web Apps

Azure Arc Enabled Servers
Azure Functions
Azure Service Fabric
Azure VM Image Builder
Azure VMware Solution
Batch
Cloud Services
Virtual Machines (incl. Reserved Instances)
Virtual Machines Scale Sets
Windows Virtual Desktop

[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.azure.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.

2.1.2 Containers

Azure Arc Enabled Kubernetes
Azure Kubernetes Service (AKS)
Azure Red Hat OpenShift
Container Instances
Container Registry

2.1.3 Networking

Application Gateway
Azure Bastion
Azure DDoS Protection
Azure DNS
Azure ExpressRoute
Azure Firewall
Azure Firewall Manager
Azure Front Door
Azure Internet Analyzer
Azure Peering Service
Azure Private Link
Azure Public IP
Azure Web Application Firewall
Content Delivery Network
Load Balancer
Network Watcher
Traffic Manager
Virtual NAT
Virtual Network
VPN Gateway
Virtual WAN

2.1.4 Storage

Azure Archive Storage
Azure Backup
Azure Data Box
Azure Data Box Edge and Gateway
Azure Data Lake Storage Gen1
Azure File Sync
Azure HPC Cache
Azure Import/Export
Azure NetApp Files
Azure Site Recovery
Azure Storage
- Archive
- Blobs (incl. Data Lake Storage Gen2)
- Disks (incl. Managed Disks)
- Files
- Queues
- Tables

2.1.5 Databases

Azure API for FHIR
Azure Cache for Redis
Azure Cosmos DB
Azure Database for MariaDB
Azure Database for MySQL
Azure Database for PostgreSQL
Azure Database Migration Service
Azure Databricks
Azure SQL
Azure Synapse Analytics
StorSimple

2.1.6 Developer Tools

Azure App Configuration
Azure DevTest Labs
Azure for Education
Azure Lab Services

2.1.7 Analytics

Azure Analysis Services
Azure Data Explorer
Azure Data Share
Azure Stream Analytics
Data Factory
Data Lake Analytics
HDInsight
Power BI Embedded

2.1.8 AI + Machine Learning

Azure Bot Service
Azure Health Bot
Azure Open Datasets
Azure Machine Learning
Cognitive Services
Machine Learning Studio (Classic)
Microsoft Genomics

2.1.9 Internet of Things

Azure Defender for IoT
Azure IoT Central
Azure IoT Hub
Azure Sphere
Azure Time Series Insights
Event Grid
Event Hubs
Notification Hubs
Windows 10 IoT Core Services

2.1.10 Integration

API Management
Logic Apps
Service Bus

2.1.11 Identity

Azure Active Directory (Free, Basic)
Azure Active Directory (Premium P1 + P2)
Azure Active Directory B2C
Azure Active Directory Domain Services
Azure Information Protection

2.1.12 Management and Governance Automation

Automation
Azure Advisor
Azure Blueprints
Azure Cost Management and Billing
Azure Lighthouse
Azure Managed Applications
Azure Migrate
Azure Monitor
Azure Policy
Azure Resource Graph
Azure Resource Manager (ARM)
Azure Service Health
Azure Service Manager (RDFE)
Cloud Shell
Microsoft Azure Portal
Schedule

2.1.13 Security

Azure Dedicated HSM
Azure Security Center
Azure Sentinel
Customer Lockbox for Microsoft Azure
Key Vault
Microsoft Azure Attestation
Microsoft Defender for Identity
Multi-Factor Authentication

2.1.14 Media

Azure Media Services

2.1.15 Web

Azure Cognitive Search
Azure Maps
Azure SignalR Service
Azure Spring Cloud Service

2.1.16 Mixed Reality

Azure Remote Rendering
Azure Spatial Anchors

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 May 2021. SCOPE Europe has been officially accredited as Monitoring Body May 2021. 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.[10]

3.2 Principles of the Verification Process

Notwithstanding the powers of and requirements set-out by the supervisory authority pursuant 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

[8] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679
[9] https://scope-europe.eu
[10] https://eucoc.cloud/en/public-register/assessment-procedure/

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; pro-actively performed by the Monitoring Body.

To the extent the Monitoring Body is not satisfied with the evidence provided by a Cloud Service Provider (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 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 Control's Catalogue, to the Monitoring Body.

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

With regards to internationally recognized 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 request for further, detailed information including potentially confidential information. Within any other Recurring Assessment, the Monitoring Body will select an appropriate share of Controls provided both that over a due period every Control will be subject to scrutiny by the Monitoring Body and aspects of increased attention as indicated e.g. by media reports, publications and actions of supervisory authorities are covered.

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 indications for appropriate implementation by the Control Guidance, then the Monitoring Body verifies the service(s) declared adherent as compliant and thereupon make 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 and 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 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 recognized 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 recognized 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 up to 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[11] and refer to the Public Register of the EU Cloud CoC[12] to enable Customers to verify the validity of adherence.

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

4.1 Fact Finding

Following the declaration of adherence of Microsoft Corporation ('**Microsoft**'), the Monitoring Body provided Microsoft with a template, requesting Microsoft 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, and are embedded in the same contractual framework.

Microsoft responded promptly supplying Monitoring Body with the filled-out template as per process. Provided information consisted of claims underpinned with references to resources made available by Microsoft to either the public or its Customers free of charge. Where applicable, underpinning evidence comprised references to specific certifications, and clauses and provisions within the respective certification report(s).

Microsoft provided convincing evidence that declared Cloud Service comprises of at the time of writing 141 individual service components that are subject to the same technical framework and share to the extent relevant for the code the same contractual framework. Monitoring Body concluded that declared Cloud Service can be flexibly configured as per Customer requirements to comprise any number and combination of the individual service components. Whichever combination and configuration the resultant service as received by the Customer is delivered under the same technical and legal framework. Therefore, Monitoring Body concludes that all declared service components form a service family, known as "Azure", declared compliant with the Code.

[11] https://eucoc.cloud/en/public-register/levels-of-compliance/
[12] https://eucoc.cloud/en/public-register/

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[13], the Monitoring Body analysed the responses and information provided by Microsoft.

Azure services including those declared adherent are validly certified to comply with ISO27001:2013, ISO27018:2014 and ISO27701:2019. Adequate statements and references were provided, and the certification status was considered regarding 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 initial submission from Microsoft which outlined how all of the requirements of the Code were met by Microsoft 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. The controls selected for this level of review were:

5.1.*, 5.2.B, 5.2.C, 5.3.C, 5.3.D, 5.3.G, 5.4.D, 5.5.E, 5.8.A, 5.12.G, 5.14.B, 6.2.H, 6.2.I and 6.2.P.

Based on the information provided by Microsoft, a follow-up request was made, for further detail on implemented measures related to Controls and respective information provided for. All follow-up responses satisfied the requests made.

4.3.2 Findings by the Monitoring Body

The assessment's priority focus was to understand the procedures safeguarding that each Customer will be provided a Cloud Service set up in a manner that is compliant with the Code, both contractually and technically. As Microsoft offers highly individualised setups per Customer, on a global scale, it was necessary to understand the existence and effectiveness of an overarching management process ensuring that such individualisation is capable to safeguard Code compliance at a minimum. Microsoft convincingly described its internal procedures, and technical architecture, safeguarding that each contract comprises of a defined minimum set of relevant provisions and that individualisations will not take adverse effects. For reasons of scalability, all service components are subject to the

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

same technical and legal framework. Internal procedures also safeguard new services or updates to existing services adhere to the same framework before being made available.

A key aspect of this assessment was Microsoft's provisions and support to its Customers discharging their GDPR compliance obligations, including data subject access requests. Microsoft provides many self-service resources for their Customers complemented with support provided through alternative means for case-by-case evaluation.

Regarding adequate sub-processor handling Microsoft clarified the requirements sub-processors must meet before they are cleared for service. Sub-processors must complete a standardized onboarding by which each sub-processor involved in the processing of Customer Personal Data must is individually assessed and cleared. The Code requires that safeguards provided by CSP must flow-down the processing chain. Microsoft goes beyond the Code's requirements by even requiring that sub-sub-processors follow the same rigorous process as sub-processors.

Monitoring Body also assessed Microsoft's due deletion of Customer Personal Data. Microsoft stated that Customer Personal Data will be ultimately deleted within 180 days of subscription expiration and/or termination as defined in the Cloud Service Agreement. As this period includes backups, required for disaster recovery, and considering the global scale at which Microsoft is providing its services, Monitoring Body has no reason to doubt that such period is in compliance with the Code's requirements and qualifies as deletion without undue delay.

5 Conclusion

Given answers by Microsoft were consistent. Where necessary Microsoft 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[14] alongside this report.

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

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

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[15].

Verification-date: May 2021 **Valid until**: May 2022

Verification-ID: 2021LVL02SCOPE116

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