SCOPE EUROPE

# Verification of Declaration of Adherence

## Declaring Company: Microsoft Corporation

EU CLOUD COC

| | |
|---|---|
| **Verification-ID** | 2021LVL02SCOPE116 |
| **Date of Approval** | May 2023 |
| **Valid until** | May 2024 |

# 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 Microsoft Azure[6]

Microsoft Azure is a cloud computing platform for building, deploying and managing cloud services through a global network for Microsoft and third-party managed data centers. 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
- App Service: API Apps
- APP Service: Mobile Apps
- APP Service: Web Apps (including Containers)
- APP Service: Static Web Apps
- Azure Arc Enabled Servers
- Azure Functions
- Azure Service Fabric
- Azure VM Image Builder
- Azure VMware solution

[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://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.

- Batch
- Cloud Services
- Virtual Machines
- Virtual Machines Scale Sets
- Windows Virtual Desktop
- Guest Configuration
- Planned Maintenance
- Service Connector
- Azure Service Manager (RDFE)

### 2.1.2 Containers

- Azure Arc Enabled Kubernetes
- Azure Kubernetes Service (AKS)
- Azure Red Hat OpenShift
- Container Instances
- Container Registry
- Azure Kubernetes Configuration Management
- Azure Container Service
- Azure Container Apps
- Azure Kubernetes Fleet Manager
- Azure Virtual Network Manager

### 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
- Microsoft Azure Peering Service
- Azure Private Link
- Azure Public IP
- Azure Web Application Firewall
- Content Delivery Network
- Load Balancer
- Network Watcher
- Traffic Manager
- Virtual Network NAT
- VPN Gateway
- Virtual WAN
- Azure Route Server
- Azure Network Function Manager

### 2.1.4 Storage

- Azure Archive Storage
- Azure Backup
- Azure Data Box
- Azure Stack Edge Service
- Azure Data Lake Storage Gen1
- Azure File Sync
- Azure HPC Cache
- Azure Import/Export
- Azure NetApp Files
- Azure Site Recovery
- Azure Storage (Cool and Premium)
  - Blobs (including Azure Data Lake Storage Gen2)
  - Disks
  - Files
  - Queues
  - Tables
  - Azure Disk Storage
- StorSimple
- Lustre as a Service

### 2.1.5 Databases

- Azure Health Data Services
- Azure Cache for Redis

- Azure Cosmos DB
- Azure Database for MariaDB
- Azure Database for MySQL
- Azure Database for PostgreSQL
- Azure Database Migration Service
- Azure SQL
- SQL Server Registry
- SAL Server Stretch Database
- Azure Arc-enabled SQL Server
- Azure Synapse Analytics
- Azure SQL Database Edge

### 2.1.6 Developer Tools

- Azure App Configuration
- Azure DevTest Labs
- Azure for Education
- Azure Lab Services
- GitHub AE
- Azure Load Testing

### 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
- Data Catalog
- Update Compliance

### 2.1.8 AI and Machine Learning

- Azure Bot Service
- Azure Health Bot
- Azure Open Datasets
- Azure Machine Learning
- Cognitive Services
- Machine Learning Studio (Classic)
- Microsoft Genomics
- AI Builder
- Azure Applied AI Services
- Cognitive Services: Anomaly Detector
- Cognitive Services: Computer Vision
- Cognitive Services: Content Moderator
- Cognitive Services: Custom Vision
- Cognitive Services: Face
- Cognitive Services: Form Recognizer
- Cognitive Services: Immersive Reader
- Cognitive Services: Language Understanding
- Cognitive Services: Personalizer
- Cognitive Services: QnA Maker
- Cognitive Services: Speech Services
- Cognitive Services: Test Analytics
- Cognitive Services: Translator
- Cognitive Services: Video Indexer
- Microsoft Autonomous Development Platform
- Microsoft Healthcare Bot
- Microsoft Bot Framework
- Cognitive Services: Metrics Advisor
- Cognitive Services: Container Platform
- Cognitive Services: Cognitive Service Platform
- Open AI Enterprise
- Azure Singularity

### 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
- Azure Digital Twins
- Microsoft Azure Peering Service
- Microsoft Cloud for Sustainability
- Device Update for IoT Hub

### 2.1.10 Integration

- API Management
- Logic Apps
- Service Bus

### 2.1.11 Identity

- Azure Active Directory (Free, Basic, Premium)
- Azure Active Directory B2C
- Azure Active Directory Domain Services
- Azure Information Protection

### 2.1.12 Management and Governance Automation

- Automation
- Azure Advisor
- Azure Blueprints
- Cost Management
- Azure Lighthouse
- Azure Managed Applications
- Azure Migrate
- Azure Monitor
- Azure Policy
- Azure Resource Graph
- Azure Resource Manager (ARM)
- Azure Service Health
- Cloud Shell
- Microsoft Azure Portal
- Scheduler
- Microsoft Purview
- Azure Signup Portal
- Application Change Analysis
- Resource Move
- Quota+ Usage blade
- Azure Managed Grafana

### 2.1.13 Security

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

### 2.1.14 Media

- Azure Media Services

### 2.1.15 Web

- Azure Cognitive Search
- Azure Maps
- Azure SignalR Service
- Azure Spring Cloud Service
- Azure Web PubSub
- Azure Fluid Relay

### 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 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 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.

[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/

## 3.3 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 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.

As this declaration is a renewal[15], the Monitoring Body requested from Microsoft a confirmation that there has been no material change to the applicable technical and organisational and contractual framework. The Monitoring Body also requested from Microsoft 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.

Microsoft 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 two 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 CoC[16], the Monitoring Body analysed the responses and information provided by Microsoft.

Microsoft’s declared services have been externally certified and audited. Microsoft 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

[15] You can access the Verification Report(s) of previous year(s) via the following link(s): Report 2022

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

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 Microsoft which outlined how all the requirements of the Code were met by Microsoft'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.E, 5.1.F, 5.1.H, 5.2.C, 5.3.D, 5.3.E, 5.3.F, 5.4.A, 5.4.C, 5.4.D, 5.4.F, 5.5.C, 5.5.D, 5.5.F, 5.7.B, 5.7.C, 5.8.A, 5.9.A, 5.9.B, 5.11.A, 5.11.B, 5.11.C, 5.12.B, 5.12.D, 5.12.E, 5.12.G, 6.1.A, 6.1.B, 6.1.C and 6.2.H.

### 4.3.2 Findings by the Monitoring Body

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

Microsoft has a privacy team in place. The privacy team, in collaboration with the Data Protection Officer (DPO), handle Customers' inquiries related to the Code, amongst other. Microsoft's employees are required to perform privacy trainings to address security and privacy practices.

In terms of sufficient Customer enablement, Customer is provided with the ability to access, extract and delete Customer Personal Data stored during the term of the Service. Customer is provided with a set period for data retrieval after the end or termination of the Cloud Service, after which Customer Personal Data is deleted by Microsoft.

The Code requires CSPs to assist Customers to respond to Data Subjects' Requests (DSRs). Microsoft provides Customer with self-service functionalities to deal with DSRs. In the event that Microsoft receives a DSR directly, the request is redirected to the Customer. Microsoft has a public guide for responding to DSRs, which includes explanation on the self-service functionalities that can be used to deal with DSRs by Customers.

The Monitoring Body assessed Microsoft's mechanisms for the transfer of personal data to third countries. Microsoft has an overarching mechanism for transfer of personal data to third Countries (i.e., SCCs). Microsoft also relies on Adequacy Decisions, when these are available.

Customers' Audit Rights, which are a standard part of Microsoft's Data Processing Agreement (DPA), were also assessed. A statement of work is, then, signed listing all detailed tasks, effort estimation and cost, when a Customer exercises its Audit Rights. Cost methodology determination is transparently communicated to Customers in the agreement.

Microsoft has a detailed public webpage on breach notification, which includes its data breach notification obligations, as well as its data breach detection and response, as well as its built-in security features. Further to this, Microsoft has a public webpage providing information on encryption, including encryption of Customer Personal Data over public networks.

Another area of focus was built around subprocessor management. Microsoft has put in place a program to ensure that subprocessors engaged during the provision of services to Customers provide, at a minimum, the same level of data protection obligations as the Cloud Service Agreement that Microsoft has concluded with its Customers. Microsoft's program verifies compliance to its data protection requirements through annual compliance cycles. New subprocessors are engaged by Microsoft only after going through the compliance check by Microsoft. A list of subprocessors is also made available to Customers through Microsoft's website, as duly indicated in the DPA.

# 5 Conclusion

The information provided 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[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 Microsoft to support the compliance of its service, the Monitoring Body grants Microsoft 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 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**: May 2023 **Valid until**: May 2024

**Verification-ID**: 2021LVL02SCOPE116

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