SCOPE EUROPE

Verification of Declaration of Adherence

Declaring Company: SAP SE

EU CLOUD COC

Verification-ID	2021LVL02SCOPE216
Date of Approval	June 2022
Valid until	June 2023

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 – was developed against Directive 95/46/EC[4] and 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 SAP Business Technology Platform (SAP BTP)[6]

SAP Business Technology Platform (SAP BTP) is a Platform as a Service (“PaaS”) comprised of four technology portfolios: database and data management, application development and integration, analytics, and intelligent technologies. The platform offers users the ability to turn data into business value, compose end-to-end business processes, and build and extend SAP applications quickly.[7]

The Cloud Service Family (SAP BTP) comprises of the following Cloud Services:

- Application Autoscaler
- Business Entity Recognition
- Data Attribute Recommendation
- Document Classification
- Document Information Extraction
- Hyperledger Fabric on SAP BTP
- SAP Cloud Identity Services - Identity Authentication
- SAP Cloud Identity Services - Identity Provisioning

[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://help.sap.com/docs/BTP?locale=en-US
[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.

- Invoice Object Recommendation
- Java Application Lifecycle Management for SAP BTP
- Java Debugging for SAP BTP
- Java Profiling for SAP BTP
- MongoDB on SAP BTP
- MultiChain on SAP BTP
- OAuth 2.0 on SAP BTP
- Object Store on SAP BTP
- PostgreSQL on SAP BTP / PostgreSQL on SAP BTP, hyperscaler option
- RabbitMQ on SAP BTP
- Redis on SAP BTP / Redis on BTP, hyperscaler option
- SAP Alert Notification service for SAP BTP
- SAP Analytics Cloud including SAP Digital Boardroom and SAP Analytics Hub
- SAP Application Logging Service for SAP BTP
- SAP ASE service
- SAP Audit Log service
- SAP Authorization and Trust Management service
- SAP BTP, ABAP environment
- SAP BTP, Cloud Foundry runtime
- SAP BTP, Kyma runtime
- SAP BTP, Neo runtime
- SAP Business Application Studio
- SAP Cloud for Energy
- SAP Cloud Identity Access Governance
- SAP Cloud Integration for data services
- SAP Cloud Portal service
- SAP Cloud Transport Management
- SAP Connectivity service
- SAP Continuous Integration and Delivery
- SAP Credential Store
- SAP Custom Domain service
- SAP Data Privacy Integration
- SAP Data Quality Management
- SAP Data Retention Manager
- SAP Data Warehouse Cloud
- SAP Destination service
- SAP Digital Manufacturing Cloud
- SAP Document Center
- SAP Document Management service, application option
- SAP Document service
- SAP Edge Services
- SAP Event Mesh
- SAP Feature Flags service
- SAP Fiori Cloud
- SAP Forms service by Adobe
- SAP Git service
- SAP HANA Cloud, SAP Adaptive Server Enterprise
- SAP HANA service for SAP BTP
- SAP HANA Spatial Services
- SAP HTML5 Application Repository service for SAP BTP
- SAP Information Collaboration Hub

- SAP Integration Suite (incl. SAP API Management, Cloud Integration, Integration Advisor, Open Connectors)
- SAP Intelligent Robotic Process Automation
- SAP Internet of Things
- SAP Job Scheduling service
- SAP Keystore service
- SAP Kubernetes Gardener
- SAP Launchpad service
- SAP Leonardo Machine Learning Foundation
- SAP Logistics Business Network, freight collaboration
- SAP Market Rates Management, Bring your own rates
- SAP Mobile services (incl. Agentry)
- SAP Monitoring service for SAP BTP
- SAP OData Provisioning
- SAP Platform Identity Provider service for SAP BTP
- SAP Software-as-a-Service Provisioning service
- SAP Solutions Lifecycle Management service for SAP BTP
- SAP Sports One
- SAP Subscription Billing
- SAP Virtual Machine service
- SAP Web Analytics
- SAP Web IDE
- SAP Workflow Management (incl. SAP Business Rules, SAP Process Visibility service, Workflow service)
- Service Ticket Intelligence
- UI Theme Designer
- UI5 flexibility for key users
- SAP Document Management service, integration option
- SAP HANA Cloud, data lake
- SAP HANA Cloud, SAP Adaptive Server Enterprise replication
- SAP HANA Cloud, SAP HANA database
- SAP Logistics Business Network, global track and trace option
- SAP Logistics Business Network, intelligent insights option
- SAP Logistics Business Network, material traceability option
- SAP Market Rates Management, Refinitiv data option
- Commercial Infrastructure Service
- SAP AI Core
- SAP AI Launchpad
- SAP API Business Hub
- SAP Asset Intelligence Network
- SAP Automation Pilot
- SAP Cloud Management service for SAP BTP
- SAP Conversational AI
- SAP Data Intelligence

- SAP Entitlement Management System
- SAP Master Data Governance, cloud edition
- SAP Master Data Integration
- SAP Multi-Bank Connectivity, Including connectivity streams for SWIFT, Financial Services Institutions (FSI) Direct member and Financial Services Institutions (FSI) Direct non-member
- SAP Personal Data Manager
- SAP Task Center
- SAP Usage Data Management service for SAP BTP
- SAP Work Zone

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 May 2021[11]. The robust and complex procedures and mechanisms can be reviewed by any third party in detail on 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

[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/

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 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 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 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 indications for 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 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[13] and refer 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 SAP (see 2.)

4.1 Fact Finding

Following the declaration of adherence of SAP SE ('**SAP**'), the Monitoring Body provided SAP with a template, requesting SAP to detail its compliance with each of the Controls of the EU Cloud CoC.

As this declaration of adherence is a renewal[15], the Monitoring Body also requested from SAP a confirmation that there has been no material change to the applicable technical and organisational framework or to the Cloud Service family.

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 SAP.

SAP's declared Cloud Services have been externally certified and audited e.g., SAP holds current SOC 2, BSI C5 and ISO 27001 for these services. The declaration of adherence referred to these reports and certifications 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 when making its assessment. Accordingly, the Monitoring Body did verify the certification and references.

4.3 Examined Controls and related findings by the Monitoring Body

4.3.1 Examined Controls

The Monitoring Body reviewed the initial submission from SAP which outlined how all the requirements of the Code were met by SAP 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

[13] https://eucoc.cloud/en/public-register/levels-of-compliance/
[14] https://eucoc.cloud/en/public-register/
[15] Previous public report can be found at: https://eucoc.cloud/fileadmin/cloud-coc/files/reports/202106_ReportVerificationDoA_SAPSE_2021LVL02SCOPE216.pdf
[16] https://eucoc.cloud/en/about/about-eu-cloud-coc/applicable-procedures/

address requests for clarifications or more detailed information. The controls selected for this level of review were: 5.1.C, 5.1.G, 5.1.H, 5.2.A, 5.2.E, 5.2.F, 5.3.D, 5.3.E, 5.3.G, 5.4.E, 5.5.E, 5.6.A, 5.7.B, 5.7.F, 5.8.A, 5.11.A-C, 5.12.C, 5.12.E, 5.12.F, 5.13.B, 5.14.E, 6.1.A, 6.2.H and 6.2.P.

4.3.2 Findings by the Monitoring Body

During the process of verification, SAP consistently prepared the Declaration of Adherence well and thoroughly. SAP promptly clarified its responses, where needed.

The focus of one of the assessments was on retention policies and schedules regarding Customer Personal Data and more particularly the personnel training on that point. Most of the retention functionalities are subject to automated deletion functionalities or are the Customers' responsibility. SAP implemented policies and procedures safeguarding that any communicated general functionalities and automatisms will not be subject to unintended modifications. Such safeguards relate to access controls to critical sources and involvement of relevant departments within the development cycle.

Furthermore, the Monitoring Body assessed the process in place that allows Customer to use its audit right and potential costs Customer would incur. SAP implemented a staggered approach, i.e., Customer shall bear the costs of any audit initiated by it, unless such audit reveals a material breach by SAP, in which case SAP will have to bear the costs. Where costs will occur to Customers, SAP confirmed that any such cost would not be excessive nor prohibitive, and following internal pre-determined criteria. In any case, costs will be mutually agreed in a dedicated audit related agreement between SAP and the respective Customer.

Another area of focus in the assessment was the implementation of appropriate procedures by SAP, as required under the Code, in relation to responding to Data Protection Supervisory Authority (SA) requests and providing assistance to Customers.

SAP implemented procedures to respond to SA requests. SAP' implemented such procedures in its overarching SAP Security Standard Incident Response and Management. SA are expected to reach out to SAP's Data Protection Officer, enabling the Data Protection and Privacy Team to ensure adequate processing of such request. Additionally, SAP has also established policies and procedures to support Customers in case of SA requests. The SAP Security Standard Incident Response and Management describes the procedure which support its capabilities to adequately react. In that context, a dedicated team will be involved and will continuously monitor customer enquiries.

The Monitoring Body paid attention to the documentation of the specific safeguards on which third country transfers are based upon and SAP's related procedures to ensure that no transfer of Customer Personal Data is performed without appropriate safeguards in place. SAP implemented Standard Contractual Clauses overarchingly.

Finally, the Monitoring Body performed an in-depth assessment on the data protection training provided to the personnel processing Customer Personal Data. SAP indicated that all personnel involved in the processing of Customer Personal Data receive adequate training as relevant for their role and job function. SAP also clarified that policies are regularly updated and, when significant changes occur, corresponding mandatory trainings are released.

5 Conclusion

The information provided by SAP were consistent. Where necessary, SAP 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 section 1. The services 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 SAP to support the compliance of its service, the Monitoring Body grants SAP with a Second Level of Compliance.

6 Validity

This verification is valid for one year. The full report consists of 12 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 2022 **Valid until**: June 2023

Verification-ID: 2021LVL02SCOPE216

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