

Verification of Declaration of Adherence

Declaring Company: SAP SE



EU
CLOUD
COC

Verification-ID 2021LVL02SCOPE216

Date of Approval June 2023

Valid until June 2024

Table of Contents

1	Verification against v2.11 of the EU Cloud CoC	3
2	List of declared services	3
2.1	SAP Business Technology Platform (SAP BTP)	3
3	Verification Process - Background	6
3.1	Approval of the Code and Accreditation of the Monitoring Body	6
3.2	Principles of the Verification Process	6
3.3	Multiple Safeguards of Compliance	6
3.4	Process in Detail	7
3.4.1	Levels of Compliance	8
3.4.2	Final decision on the applicable Level of Compliance	9
3.5	Transparency about adherence	9
4	Assessment of declared services by SAP (see 2.)	9
4.1	Fact Finding	9
4.2	Selection of Controls for in-depth assessment	10
4.3	Examined Controls and related findings by the Monitoring Body	10
4.3.1	Examined Controls	10
4.3.2	Findings by the Monitoring Body	11
5	Conclusion	12
6	Validity	12

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 Group³ (**'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/EC⁴ 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 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:

- SAP BTP Runtime:
 - SAP BTP, Neo runtime
 - SAP BTP, Cloud Foundry runtime
 - BTP, Kyma runtime
- SAP BTP, ABAP environment
- SAP AI Core
- SAP AI Launchpad
- SAP Alert Notification service for SAP BTP
- SAP Analytics Cloud including SAP Digital Boardroom and
- SAP Analytics Hub
- SAP API Business Hub
- SAP Application Logging Service for SAP BTP
- SAP ASE service
- SAP Audit Log Service

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.

- SAP Authorization and Trust Management service
- SAP Automation Pilot
- SAP Business Network for Logistics:
 - SAP Business Network Freight Collaboration
 - SAP Business Network Global Track and Trace
 - SAP Business Network Intelligent Insights
 - SAP Business Network Material Traceability
- SAP Business Network Asset Collaboration
- SAP Business Application Studio
- SAP Batch Release Hub for Life Sciences
- SAP Cloud Appliance Library
- SAP Cloud for Energy
- SAP Cloud Identity Access Governance
- SAP Cloud Identity Services - Identity Authentication
- SAP Cloud Identity Services - Identity Provisioning
- SAP Cloud Integration for data services
- SAP Cloud Management service for SAP BTP
- SAP Cloud Portal service
- SAP Cloud Transport Management
- SAP Connectivity service
- SAP Content Agent service
- SAP Continuous Integration and Delivery
- SAP Conversational AI
- SAP Credential Store
- SAP Custom Domain service
- SAP Data Custodian
- SAP Data Intelligence
- SAP Data Privacy Integration
- SAP Data Quality Management
- SAP Data Retention Manager
- SAP Datasphere, incl. SAP BW Bridge
- SAP Destination service
- SAP Digital Manufacturing Cloud
- SAP Document Center
- SAP Document Management:
 - SAP Document Management service, integration option
 - SAP Document Management service, application option
- SAP Document service
- SAP Entitlement Management
- SAP Event Mesh
- SAP Feature Flags service
- SAP Fiori Cloud
- SAP Forms service by Adobe
- SAP Git service
- SAP Graph
- SAP HANA Cloud:
 - SAP HANA Cloud, data lake
 - SAP HANA Cloud, SAP HANA database
- 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:
 - SAP API Management
 - Cloud Integration
 - Integration Advisor
 - Open Connectors
- SAP Intelligent Robotic Process Automation

- SAP Job Scheduling service
- SAP Keystore service
- SAP Landscape Management Cloud
- SAP Launchpad service
- SAP Leonardo Machine Learning Foundation
- SAP Malware Scanning Service
- SAP Market Communication for Utilities
- SAP Market Rates Management:
 - SAP Market Rates Management, Bring your own rates
 - SAP Market Rates Management, Refinitiv data option
- SAP Master Data Governance, cloud edition
- SAP Master Data Integration
- SAP Mobile Services (incl. Agency)
- SAP Monitoring service for SAP BTP
- SAP Multi-Bank Connectivity
- SAP OData Provisioning
- SAP Personal Data Manager
- SAP Platform Identity Provider service for SAP BTP
- SAP Private Link Service
- SAP Service Manager
- SAP Software-as-a-Service Provisioning service
- SAP Solutions Lifecycle Management service for SAP BTP
- SAP Sports One
- SAP Subscription Billing
- SAP Task Center
- SAP Usage Data Management service for SAP BTP
- SAP Virtual Machine service
- SAP Web IDE
- SAP Workflow Management:
 - SAP Business Rules
 - SAP Process Visibility service
 - Workflow service
- SAP Work Zone
- Application Autoscaler
- Business Entity Recognition
- Data Attribute Recommendation
- Document Classification
- Document Information Extraction
- Invoice Object Recommendation
- Java Application Lifecycle Management for SAP BTP
- Java Debugging for SAP BTP
- Java Profiling for SAP BTP
- MongoDB 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
- Service Ticket Intelligence
- UI Theme Designer
- UI5 flexibility for key users

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 GDPR⁸.

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/bvba⁹.

The Code has been officially approved in May 2021¹⁰. SCOPE Europe has been officially accredited as Monitoring Body in May 2021¹¹. 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.

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

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/>

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 Mark¹³ and referring to the Public Register of the EU Cloud CoC¹⁴ 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 is a renewal¹⁵, the Monitoring Body requested from SAP a confirmation that there has been no material change to the applicable technical and organisational and contractual framework. The Monitoring Body also requested from SAP 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

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): [External Report 2022](#)

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.

SAP 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's 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 CoC¹⁶, the Monitoring Body analysed the responses and information provided by SAP.

SAP's declared services have been externally certified and audited. SAP 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 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 SAP which outlined how all the requirements of the Code were met by SAP'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, 5.2.A, 5.2.D, 5.3.B, 5.4.E, 5.5.E, 5.9.B, 5.11.A, 5.11.B, 5.11.C, 5.12.C, 5.13.B, 5.14.F, 6.1.C and 6.2.H.

¹⁶ <https://eucooc.cloud/en/about/about-eu-cloud-coc/applicable-procedures/>

4.3.2 Findings by the Monitoring Body

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

A first area of focus was around SAP processing personal data only on the written instructions of Customer. SAP confirmed that instructions from Customers are standardised and customer-specific deviations are limited to necessary exceptions only. Instructions from Customers are documented and an integral part of the contractual agreements. Implementation of these instructions is ensured by providing Customers the technical means to tailor their respective Cloud Service to their own needs.

Another area of focus was built around subprocessor management. SAP has a defined mechanism to notify Customers of changes in subprocessors. The timelines for objection and/or exercising an alternative option, as well as the means to do so were confirmed by SAP's contractual documents. In the same vein, flow-down mechanisms are implemented. This includes contractual obligations of subprocessors to adhere to the same standards of data processing as SAP. Additionally, SAP makes available to its Customers general information about existing subprocessors through the SAP Trust Center.

Regarding third country transfers, SAP implemented safeguards as provided by Chapter V GDPR. SAP has implemented the Standard Contractual Clauses (SCCs), which are used as a transfer mechanism to safeguard Customer Personal Data. Data Transfer Factsheets are made available to Customers through the SAP Trust Center which maps the countries where Customer Personal Data are transferred to, for transparency purposes.

Another area of assessment has been the enablement of Customers, with respect to Customers responding to Data Subject Requests. Customers are provided with the possibility to do so through self-service functionalities. Relevant documentation providing an overview on these functionalities are made available for the respective service. Where Customers require more information not covered by the self-service functionalities provided, Customers may reach out to SAP either via standard support channels or the DPO contact.

The Monitoring Body also assessed Customers' Audit Rights. SAP's reports and certifications are made available through the SAP Trust Center. Audit Rights are a standard part of SAP's DPA and operationalisation of those rights are ensured through a documented procedure. The assessment also focused on the possibility for Customers to request additional evidence of compliance. SAP provided the Monitoring Body with an explanation on the relevant communication channels through which Customers can request additional evidence of compliance, beyond exercising their audit rights.

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 1. The service(s) will be listed in the Public Register of the EU Cloud CoC¹⁷ 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 CoC¹⁸.

Verification-date: June 2023

Valid until: June 2024

Verification-ID: 2021LVL02SCOPE216

¹⁷ <https://euococ.cloud/en/public-register/>

¹⁸ <https://euococ.cloud/en/public-register/>