SCOPE EUROPE

Verification of Declaration of Adherence

Declaring Company: SAP SE

Verification-ID	2025LVL02SCOPE5423
Date of Approval	March 2025
Valid until	March 2026

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 (**'CSPs'**) – 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 SAP S/4HANA Cloud Public Edition[6]

SAP S/4HANA Cloud, public edition is a real-time enterprise resource management suite for digital business available as software-as-a-service. It is built on our advanced in-memory platform, SAP HANA, and offers a personalized, consumer-grade user experience with SAP Fiori built on the in-memory platform SAP HANA. SAP S/4HANA Cloud, public edition is also already connected to business networks and company-internal collaboration networks and prepared for the Internet of things.[7]

2.2 SAP Advanced Financial Closing[8]

SAP Advanced Financial Closing (AFC) is a cloud application for planning, processing, monitoring, and analyzing financial closing tasks for the entities in the customer's financial backend.[9]

---

[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.sap.com/products/erp/s4hana.html
[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.
[8] https://www.sap.com/products/financial-management/advanced-financial-closing.html
[9] **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.

2.3 SAP Group Reporting Data Collection

SAP Group Reporting Data Collection is a cloud-based solution that helps customers collect financial data, non-financial and comments into SAP S/4HANA Finance for group reporting.[10]

2.4 SAP Business ByDesign[11]

SAP Business ByDesign (ByD) is a cloud-based Software-as-a-Service (SaaS) ERP offering for mid-market companies and subsidiaries, powered by SAP HANA. With SAP Business ByDesign, organizations can manage their entire business with a single cloud ERP solution. Ideally suited for upper mid-market companies and subsidiaries of large corporations, this complete and integrated Software as a Service (SaaS) suite supports financials, human resources, sales, procurement, customer service, supply chain management, and more.[12]

2.5 SAP Project and Resource Management[13]

SAP Project and Resource Management is a set of modular cloud services which enable customers to orchestrate projects and teams across organizations and locations in order to deliver successful projects.[14]

2.6 SAP Integrated Business Planning[15]

SAP Integrated Business Planning is SAP's platform for real-time and integrated planning, built on SAP HANA, utilizing HANA's Analytical features to the maximum. SAP Integrated Business Planning is being developed to deliver integrated, unified planning across Sales and Operations, Demand, Inventory, Supply and Response planning, as well as the Supply Chain Control Tower for dashboard analytics and monitoring.[16]

---

[10] **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.
[11] https://www.sap.com/products/erp/business-bydesign.html
[12] **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.
[13] https://www.sap.com/products/scm/project-resource-management.html
[14] **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.
[15] https://www.sap.com/products/scm/integrated-business-planning.html
[16] **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.

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[17].

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 srl/bv[18].

The Code has been officially approved in May 2021[19]. SCOPE Europe has been officially accredited as Monitoring Body in May 2021[20]. 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.[21]

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

[17] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679
[18] https://scope-europe.eu
[19] https://www.gegevensbeschermingsautoriteit.be/publications/decision-n05-2021-of-20-may-2021.pdf
[20] https://www.gegevensbeschermingsautoriteit.be/publications/decision-n-06-2021-of-20-may-2021.pdf
[21] 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 Mark[22] and referring to the Public Register of the EU Cloud CoC[23] 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.

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 (i.e., technical framework), and are embedded in the same organisational and contractual framework.

[22] https://eucoc.cloud/en/public-register/levels-of-compliance/
[23] https://eucoc.cloud/en/public-register/

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. SAP provided information illustrating the actual structure of the services declared adherent and describing the technical, organisational and contractual framework. Selection of Controls for in-depth assessment

Following the provisions of the Code and the Assessment Procedure applicable to the EU Cloud CoC[24], the Monitoring Body analysed the responses and information provided by SAP.

SAP's declared services have been externally certified and audited. SAP holds a current 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 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.

4.2 Examined Controls and related findings by the Monitoring Body

4.2.1 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, 5.3.A, 5.3.C, 5.4.D, 5.5.B—D, 5.7.C, 5.7.F, 5.8.A, 5.10.B, 5.11.B, 5.12.E-G, 5.13.A, and 6.1.C.

4.2.2 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.

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

The Monitoring Body verified that declared Cloud Services qualify both as Cloud Service under the Code and as Cloud Service Family. Related to the Monitoring Body's requests (see section 4.1), SAP provided information outlining the structure of the services, contractual and supporting documents enabling the Monitoring Body to better understand SAP's service offerings. SAP provided explicit confirmation that all Cloud Services declared adherent belong to the same Cloud Service Family.

The assessment involved the subprocessor management process. Based on the information provided by SAP, a review process is in place to ensure that SAP only engages subprocessors that can provide sufficient guarantees of compliance with GDPR. Moreover, SAP obtains a general authorization of the Customer prior to the processing of Customer Personal Data when engaging subprocessors.

Related to third country transfers, SAP continually monitors international processing of data, including the applicability of existing adequacy decisions. Furthermore, SAP indicated that an up-to date and accurate Record of Processing Activities (ROPA) is available for Customers to access in accordance with Article 30.2 GDPR.

When it comes to Customer's Audit Rights, SAP makes available to its Customers independent third-party audit reports and certifications, and the CSP confirmed that Customers are able to request additional evidence. Additionally, SAP confirmed that procedures regarding Customer-requested audits are documented and transparently communicated to the Customer.

Another area of the assessment has been personnel training and awareness. SAP has established regular trainings in organizational policies and procedures for its employees involved in the processing of Customer Personal Data. Moreover, SAP confirmed that the trainings are tailored to the processing of data and subject to periodic reviews.

Based on the information provided by the CSP, SAP has established documented procedures assisting the Customer for fulfilling data subject requests. In the same vein, SAP has established documented procedures to respond to requests by supervisory authorities ensuring that such responds take place in due time and ap propriate detail and quality.

Data breach notification and reporting obligations have been in the scope of the assessment. In this vein, SAP confirmed that policies and procedures are implemented to identify and handle data breaches without undue delay, if any such breach should happen.

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 CoC[25] 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 11 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[26].

Verification-date: March 2025 **Valid until**: March 2026

Verification-ID: 2025LVL02SCOPE5423

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