Verification of Declaration of Adherence

Declaring Company: SAP SE

Verification-ID	2025LVL02SCOPE5423
Date of Approval	March 2026
Valid until	March 2027

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' or 'Code')**[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/4 HANA 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.

2.7 SAP Asset Performance Management[17]

SAP Asset Performance Management is an application which is designed to help asset owners, managers, plant managers, and reliability engineers measure and improve the performance of their assets and optimize their maintenance strategies.[18]

2.8 SAP Integrated Product Development[19]

SAP Integrated Product Development is a cloud solution that enables customers to digitally orchestrate their product development, from design to operate, resulting in reduced time to market, higher R&D return on investment, higher margins, and reliable product launches.[20]

2.9 SAP Print Service[21]

The SAP Print service offers printing functionality and lets you monitor the printing status. Customers can send documents to the print service and then print out documents using a physical printer. The documents are stored temporarily, so they can be printed later and control the output from the printer.[22]

2.10 SAP Risk and Assurance Management[23]

SAP Risk and Assurance Management is a controls/checks execution, monitoring, reporting and management solution, running on SAP Business Technology Platform. It provides a centralized view across SAP S/4HANA Cloud Private and Public Editions and ECC, for control performance, status and adequacy. It supports meeting statutory compliance regulations yet reduces the overall cost of compliance, tax risk, and improves investment and liability management.[24]

---

[17] https://www.sap.com/products/scm/apm.html
[18] **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.
[19] https://www.sap.com/products/scm/integrated-product-development.html
[20] **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.
[21] https://www.sap.com/products/technology-platform/print-service.html
[22] **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.
[23] https://www.sap.com/products/financial-management/financial-compliance-management.html
[24] **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.

2.11 SAP Document Reporting Compliance, Cloud Edition[25]

SAP Document and Reporting Compliance, cloud edition is a SaaS application based on SAP Business Technology Platform (BTP) helps customers to exchange invoices and related documents in electronic format with authorities and business partners. The service includes connectors part of source systems (SAP Document and Reporting Compliance in SAP ERP and SAP S/4HANA, Ariba, Concur, SAP BusinessOne, SAP Business ByDesign).[26]

2.12 SAP Digital Currency Hub[27]

SAP Digital Currency Hub enables customers to make and receive payments with digital currencies as well as hold digital currencies without an intermediary. By leveraging digital money pegged to an underlying fiat currency, such as the US Dollar or Euro, and using blockchain technology as the underlying settlement layer, it empowers businesses to perform fast, affordable, and reliable transactions. It is a software-as-a-service solution that can complement ERP systems.[28]

2.13 SAP CPQ[29]

SAP CPQ (Configure, Price, and Quote) is a highly configurable system designated to help sales representatives to configure products, apply pricing and generate quotes. The core process (configuring, pricing, and quoting) in SAP CPQ can be enhanced with advanced features as needed, depending on the customer's business model and what they wish to accomplish with SAP CPQ.[30]

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[31].

---

[25] https://www.sap.com/products/financial-management/document-reporting-compliance.html
[26] **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.
[27] https://www.sap.com/products/financial-management/digital-currency-hub.html
[28] **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.
[29] https://www.sap.com/products/financial-management/cpq.html
[30] **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.
[31] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

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[32].

The Code has been officially approved in May 2021[33]. SCOPE Europe has been officially accredited as Monitoring Body in May 2021[34]. 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.[35]

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 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

---

[32] https://scope-europe.eu
[33] https://www.gegevensbeschermingsautoriteit.be/publications/decision-n05-2021-of-20-may-2021.pdf
[34] https://www.gegevensbeschermingsautoriteit.be/publications/decision-n-06-2021-of-20-may-2021.pdf
[35] https://eucoc.cloud/en/public-register/assessment-procedure/

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[36] and referring to the Public Register of the EU Cloud CoC[37] 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 renewal[38], 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 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.

[36] https://eucoc.cloud/en/public-register/levels-of-compliance/
[37] https://eucoc.cloud/en/public-register/
[38] You can access the Verification Report of previous year via the following link: SAP - Verification Report - (2025)

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 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[39], 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 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.

4.3 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.E, 5.1.F, 5.2.B, 5.2.E, 5.2.F, 5.2.G, 5.3.B, 5.3.C, 5.3.E, 5.4.A, 5.4.B, 5.5.B, 5.5.E, 5.7.A, 5.7.B, 5.7.F, 5.8.A, 5.8.B, 5.11.B, 5.12.A, 5.12.D, 5.12.E, 5.12.G, 5.13.B, 5.14.E and 6.1.C.

[39] https://eucoc.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.

The Monitoring Body assessed SAP's policies related to data retention and disposal which establish the requirements for return and deletion of Customer Personal Data. SAP provided an overview on the means for data retrieval, as well as specific procedures for data deletion. In the same vein, the CSP explained how it maintains an appropriate media disposal and data wiping procedure governing storage media no longer in use.

Customers' Audit Rights were also assessed. SAP has adopted a staggered approach, which ensures that existing audit reports are provided to Customers at a first step through the CSP's Trust Center. As a second step, Customers are provided with the possibility to request additional information and as a final step, audit requests can be made by the Customers. SAP provided the Monitoring Body with an overview of the internal process for Customer Audits.

In addition to this, the assessment focused on the possibility for Customers to request additional evidence of compliance and that related communication channels are adequately communicated to Customers. SAP provided the Monitoring Body with an explanation on the relevant communication channels through which Customers may request additional evidence of compliance, beyond exercising their audit rights.

The Monitoring Body also assessed the data breach notification and reporting obligations. Based on the information provided by SAP, relevant policies and procedures are in place to identify and handle data breaches without undue delay, if any such breach were to happen. In line with these policies and procedures, SAP determines whether a security breach potentially resulted into a data breach and ensures that Customers are notified, as provided by the GDPR. Data breach reporting obligations are included in the contractual documentation with Customers and form an integral part of the implemented procedures.

Furthermore, SAP maintains documented procedures to assist Customers with their Data Protection Impact Assessment ("DPIA"). While this is included as a contractual obligation, SAP also maintains procedures and policies providing details on how to support its Customers in this regard. In the same vein, information classification procedures are implemented to ensure that information provided to a Customer for their DPIA does not create a security risk for the CSP.

5 Conclusion

The information provided by SAP was 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[40] alongside this report.

In accordance with sections 3.4.1.13.4.1.2 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 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[41].

Verification-date: March 2026 **Valid until**: March 2027

Verification-ID: 2025LVL02SCOPE5423

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