SCOPE EUROPE

Verification of Declaration of Adherence

Declaring Company: SAP SE

Verification-ID	2025LVL02SCOPE5425
Date of Approval	September 2026
Due Date	September 2027

Table of Contents

1 Verification against v2.12 of the EU Cloud CoC 3

2 List of declared services 3

2.1 SAP Ariba 3

2.1.1 SAP Ariba Procurement 3

2.1.2 SAP Ariba Strategic Sourcing 4

2.1.3 SAP Ariba Category Management 4

3 Verification Process - Background 4

3.1 Approval of the Code and Accreditation of the Monitoring Body 4

3.2 Principles of the Verification Process 4

3.3 Multiple Safeguards of Compliance 5

3.4 Process in Detail 5

3.4.1 Levels of Compliance 6

3.4.2 Final decision on the applicable Level of Compliance 7

3.5 Transparency about adherence 8

4 Assessment of declared services by SAP (see 2.) 8

4.1 Fact Finding 8

4.2 Selection of Controls for in-depth assessment 9

4.3 Examined Controls and related findings by the Monitoring Body 9

4.3.1 Examined Controls 9

4.3.2 Findings by the Monitoring Body 9

5 Conclusion 11

6 Validity 11

1 Verification against v2.12 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 2.12 ("**v2.12**")[2] as of September 2026.

The EU Cloud CoC was originally drafted by the Cloud Select Industry Group[3] ("**C-SIG**") as the C-SIG Code of Conduct on data protection for Cloud Service Providers ("**CSPs**") and was developed against Directive 95/46/EC[4], incorporating feedback by the European Commission, as well as Working Party 29. Following extensive revisions of earlier versions of Code and further developing the substance of the Code (v2.12) and its provisions has been aligned to the European General Data Protection Regulation ("**GDPR**")[5].

2 List of declared services

2.1 SAP Ariba [6]

SAP Ariba is a comprehensive strategic sourcing and procurement solutions that support the entire sourcing, contracting, and spend analysis lifecycle across all spend types. These solutions integrate procure-to-pay and procure-to-order capabilities, enabling organizations to define and manage purchasing categories effectively.[7]

2.1.1 SAP Ariba Procurement

SAP Ariba Procure-to-Pay (P2P) and Procure-to-Order (P2O) software solutions streamline the entire procurement process—from requisitioning and ordering to invoicing and payment.[7]

- Buying
- Guided Buying
- Buying and Invoicing
- Snap
- Spot Buy Capability
- Catalog
- Procurement Planning
- Central Invoice Management

[1] https://eucoc.cloud
[2] https://eucoc.cloud/get-the-code
[3] https://digital-strategy.ec.europa.eu/en/news/cloud-select-industry-group
[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://service.ariba.com/
[7] **NOTE:** The content for the service description has been provided by the CSP and does not reflect any opinion of or assessment by the Monitoring Body.

2.1.2 SAP Ariba Strategic Sourcing

SAP Ariba Strategic Sourcing Solutions enable organizations to manage the complete sourcing lifecycle—including sourcing events, contract management, and spend analysis—across all types of spend.[7]

- Sourcing
- Contracts
- Spend Analysis
- Supplier Risk
- Supplier Lifecycle Management
- Supplier Information & Performance Management
- Supplier Lifecycle & Performance

2.1.3 SAP Ariba Category Management

SAP Ariba Category Management empowers organizations to define and manage purchasing categories effectively. It delivers actionable market intelligence, deep category insights, and a suite of tools and templates to help develop and implement strategic category plans.[7]

3 Verification Process - Background

V2.12 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 SRL[9].

The Code has been officially approved in May 2021[10]. SCOPE Europe has been officially accredited as Monitoring Body in May 2021[11]. The robust and complex procedures and mechanisms can be reviewed by any third-party in detail at the website of the EU Cloud CoC alongside a short summary thereof.[12]

3.2 Principles of the Verification Process

Notwithstanding the powers of and requirements set out by the supervisory authority pursuant to Article 41 GDPR, the Monitoring Body will assess whether a Cloud Service (family), that has been declared adherent to the Code, is compliant with the requirements of the Code – especially as laid

[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/

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 (family) 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 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 infrastructure, 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 (family) 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 (family) declared adhered as compliant and thereupon, makes them subject to continuous monitoring.

3.4.1 Levels of Compliance

V2.12 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 (family) and confirms that the Cloud Service (family) 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 (family) 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 (family) declared adherent and which were based upon internationally recognised standards. 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 (family) 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

Similar 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 (family) 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 (family) adherent to the EU Cloud CoC must transparently communicate its adherence by both using the appropriate Compliance Mark[13] and referring to the Public Register of the EU Cloud CoC[14] to enable Customers to verify the validity of adherence.

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[15], the Monitoring Body requested from SAP a confirmation that there has been no material change to the applicable technical infrastructure, as well as organisational and contractual frameworks. The Monitoring Body also requested from SAP a comparison of the Cloud Services declared last year and the Cloud Services to be declared 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 (e.g., EOL, merging, etc.). 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 infrastructure, as well as overarching organisational and contractual frameworks as the original Cloud Services.

SAP promptly responded. 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.

[13] https://eucoc.cloud/en/public-register/levels-of-compliance/
[14] https://eucoc.cloud/en/public-register/
[15] You can access the Verification Report of previous year via the following link: SAP (Ariba) - Verification Report – (2025)

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 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.A, 5.1.C-F, 5.2.E, 5.3.B, 5.3.E, 5.5.A, 5.5.E, 5.7.B, 5.7.D-F, 5.8.A-B, 5.10.A-B, 5.12.A, 5.12.D, 5.13.B and 6.1.C.

4.3.2 Findings by the Monitoring Body

During the process of verification, SAP provided responses that were considered detailed. There was no 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 frameworks. Where additional Cloud Services were added, SAP provided explicit confirmation that such Cloud Services belong to the same Cloud Service Family.

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

SAP confirmed that a Cloud Service Agreement ("CSA") is in place with Customers, incorporating the data protection obligations under the GDPR as a minimum. The CSA determines the responsibilities of the Customers and the CSP regarding the security measures, the terms under which the Customer Personal Data shall be processed, and the scope of Customer's instructions.

SAP indicated that its adherence to the Code is communicated to its personnel and that the latter is aware of the adherence to the Code in order to adequately handle Customer-related inquiries. The CSP also ensures that all personnel involved in the processing of Customer Personal Data receives mandatory data protection and privacy training. Security and privacy training is relevant to the personnel's role and job function in relation to the Cloud Services. The training programme is subject to timely reviews in terms of its content, participation, as well as its quality and effectiveness.

The assessment involved the subprocessor management process. Based on the information provided, SAP makes available to the Customer, through its contractual documentation and dedicated subprocessors webpage, general information regarding its existing subprocessors and the jurisdictions applicable to the processing of Customer Personal Data. Moreover, SAP has a defined mechanism to notify Customers of changes in subprocessors. The timeline for the Customers to object to the appointment of new subprocessors and/or to exercise an alternative option was confirmed by the CSP.

The Monitoring Body also assessed Customers' Audit Rights. The CSP makes certificates, attestations and reports readily available on its website. In the same vein, SAP makes available to Customers an executive summary of independent third-party audits through its Trust Center. In addition, SAP provided the Monitoring Body with an overview of its methodology to determine the costs of Customer-mandated audits. Based on the information presented to the Monitoring Body, there was no indication that such costs are prohibitive or excessive.

When it comes to assistance provided to the Customers, information with regards to data formats, processes, technical requirements and timeframes of retrieving the entrusted Customer Personal Data is provided to Customers in the relevant contractual documents and in CSP's Trust Center. Customers can make use of various self-service capabilities to access all relevant information and deal with data subject requests ("DSRs"), including data retention, deletion, and the retrieval and export of Customer Personal Data. Additionally, SAP has established documented procedures to assist Customers with Data Protection Impact Assessments ("DPIAs") and has implemented relevant internal policies and procedures to ensure that the information provided to Customers in support of their DPIAs does not create a security risk for the CSP.

SAP's records of processing activities ("ROPA") built another area of focus. SAP confirmed that it maintains an up-to-date and accurate ROPA in its capacity as a Processor, which includes the relevant information as per Art. 30.2 GDPR. As a part of the self-service capabilities offered by SAP, Customers are enabled to provide and update their information that pertains to the completion and relevancy of the ROPA.

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[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 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[18].

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

Verification-ID: 2025LVL02SCOPE5425

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