

Verification of Declaration of Adherence

Declaring Company: SAP SE



EU
CLOUD
COC

Verification-ID 2024LVL02SCOPE5421

Date of Approval August 2024

Valid until August 2025

Table of Contents

1	Verification against v2.11 of the EU Cloud CoC	3
2	List of declared services	3
2.1	SAP SuccessFactors Employee Central Payroll	3
2.2	SAP SuccessFactors HCM Suite	3
3	Verification Process - Background	5
3.1	Approval of the Code and Accreditation of the Monitoring Body	5
3.2	Principles of the Verification Process	5
3.3	Multiple Safeguards of Compliance	5
3.4	Process in Detail	6
3.4.1	Levels of Compliance	7
3.4.2	Final decision on the applicable Level of Compliance	8
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	10
5	Conclusion	11
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

1.1 SAP SuccessFactors Employee Central Payroll⁶

SAP SuccessFactors Employee Central Payroll – Help ensure accurate payroll calculation, monitor payroll processes, and improve organizational results.⁷

1.2 SAP SuccessFactors HCM Suite⁸

The SAP SuccessFactors HCM system provides the following solutions⁷:

- **SAP SuccessFactors Workforce Analytics and Planning** – SAP SuccessFactors Workforce Analytics and Planning provides standardized HR metrics and helps organizations to analyse and forecast workforce trends, including headcount, hiring and turnover.
- **SAP SuccessFactors Learning** – SAP SuccessFactors Learning combines formal, social, and extended learning content management and reporting. It facilitates compliance training and reporting to help organizations meet regulatory requirements.
- **SAP Jam** – SAP Jam is an enterprise collaboration platform that allows users to collaborate, and share and find information, including videos and screen captures. Jam also includes support for Microsoft Office documents and PDFs, which allows for discovery and commenting, even from a mobile phone or tablet. Additional features including polling, activity

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 [Payroll Management System | SAP SuccessFactors Employee Central Payroll](#)

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 [SAP SuccessFactors | Human Capital Management | Cloud HR Software](#)

feeds, and public and private groups which enable employees to crowd source questions, discuss and debate ideas, and keep processes on schedule.

- **SAP SuccessFactors Recruiting** — SAP SuccessFactors Recruiting helps organizations to source talent, track job applicants and manage candidate relationships. It provides the ability to access global job boards, build talent pools to find past applicants and build branded career sites.
- **SAP SuccessFactors Onboarding** — SAP SuccessFactors Onboarding allows managers to leverage a step-by-step wizard to create a personalized onboarding plan for new hires. Accessing an onboarding portal, new hires connect with recommended tools, content, and colleagues. SAP SuccessFactors Onboarding also supports the cross-boarding and off-boarding of employees.
- **SAP SuccessFactors Employee Central** — SAP SuccessFactors Employee Central provides a central location for all employee data to help HR measure the contribution of the workforce to business results. SAP SuccessFactors Employee Central offers organizational management, global benefits administration, and team absence tracking. The solution is localized in 100+ countries.
- **SAP SuccessFactors Employee Central Service Center** — SAP SuccessFactors Employee Central Service Center is an HR help desk solution. Employees submit service tickets to receive assistance and information from HR service agents.

- **SAP SuccessFactors Time Tracking** — SAP SuccessFactors Time Tracking supports an organization's time administration strategy and enables employees to submit timesheets. The solution includes clock-in and clock-out, time account payouts and automated calculations and approvals.
- **SAP Work Zone for HR** — SAP Work Zone for HR is a digital workplace that provides access to relevant business applications and processes, information, and communication with a unified entry point for work. The solution guides employees through complex, end-to-end processes that span across multiple business applications.
- **SAP SuccessFactors Performance and Goals** — SAP SuccessFactors Performance and Goals provides a means to manage employee performance and tracks the performance review process and ongoing performance conversations between employees and managers.
- **SAP SuccessFactors Compensation** — SAP SuccessFactors Compensation enables planning and management of various types of compensation programs, including salary, merit increases, market adjustments, lump sum payments and other discretionary pay components.
- **SAP SuccessFactors Succession and Development** — SAP SuccessFactors Succession and Development enables users to create and maintain development plans that are integrated with learning recommendations. The solution supports personalized plans with specific, measurable and time-framed (SMART) goals and supporting action items.

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 GDPR⁹.

1.3 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/bvba¹⁰.

The Code has been officially approved in May 2021¹¹. SCOPE Europe has been officially accredited as Monitoring Body in May 2021¹². 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.¹³

3.1 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.

3.2 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

⁹ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679>

¹⁰ <https://scope-europe.eu>

¹¹ <https://www.gegevensbeschermingsautoriteit.be/publications/decision-n05-2021-of-20-may-2021.pdf>

¹² <https://www.gegevensbeschermingsautoriteit.be/publications/decision-n-06-2021-of-20-may-2021.pdf>

¹³ <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.

3.3 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.

3.3.1 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.

3.3.1.1 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.

3.3.1.2 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.

3.3.1.3 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.

1.3.1 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.

3.4 Transparency about adherence

Each service adherent to the EU Cloud CoC must transparently communicate its adherence by both using the appropriate Compliance Mark¹⁴ and referring to the Public Register of the EU Cloud CoC¹⁵ to enable Customers to verify the validity of adherence.

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

1.4 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.

¹⁴ <https://eucoc.cloud/en/public-register/levels-of-compliance/>

¹⁵ <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.

4.1 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 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 27001 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 3.3, 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-C, 5.1.F, 5.1.H, 5.2.D, 5.2.F-G, 5.3.F, 5.5.E, 5.8.B, 5.12.D, 5.12.G, 5.14.D, 5.14.F and 6.1.C.

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

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.

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 1.4), 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 Monitoring Body particularly focused on verifying the establishment of Cloud Service Agreement ('CSA') describing the scope covering Customer Personal Data that might be processed by the Cloud Service Provider. SAP indicated to have in place a CSA with its Customers, incorporating the obligations as required by the Code, including the definition of the roles and responsibilities of both the CSP and the Customer with respect to security measures and detailed descriptions of the processing activities.

Furthermore, SAP processes Customer Personal Data according to the Customer's instructions as outlined in the CSA. SAP affirmed that relevant information is made accessible to Customers to ensure lawful data processing and mechanisms for data retention and deletion, aligned with Customer requirements, are implemented. Additionally, SAP identified to provide necessary support and ensures that processing activities are conducted in accordance with Customer's instructions.

Another aspect of the assessment involved SAP's subprocessors' management. Based on the information provided, SAP implemented policies and procedures ensuring that SAP only engages subprocessors that will provide sufficient guarantees of compliance with GDPR. SAP's procedures require the obtention of prior written authorization from Customers before engaging subprocessors. SAP established a notification mechanism to inform Customers about additions or replacements concerning subprocessors.

The Monitoring Body assessed Customer Audit Rights and CSP's obligation to provide summaries of independent third-party audits, certification reports to Customers and allow for an on-site inspection. SAP's has defined, documented, and communicated procedures regarding Customer-requested au-

dits. SAP provided information that it ensures that costs related to audits are not excessive or prohibitive. SAP guarantees to give necessary access to information and to maintain appropriate confidentiality standards.

In relation to records of processing activities ('ROPA'), SAP assured to maintain an up-to-date and accurate records of processing activities conducted on behalf of Customers. The assurance included elements allowing the Monitoring Body to understand that the ROPA includes necessary information as per Article 30 (2) GDPR, such as the name and contact details of Customers, categories of processing activities, and details of subprocessors. SAP implemented procedures enabling Customers to provide the necessary information for maintaining these records.

The Monitoring Body has assessed procedures with regards to the confidentiality obligations under the Code. SAP confirmed that all personnel involved in processing of Customer Personal Data are subject to appropriate confidentiality obligations, which continue after the end of employment or termination of contracts. SAP indicated documented policies and procedures to enforce these confidentiality obligations and provides regular data protection and awareness training to relevant personnel, ensuring that the processing of Customer Personal Data is conducted in accordance with the Code and Customer's instructions.

Upon termination of the CSA, SAP affirmed to provide Customers with the capability to retrieve their personal data promptly and without hindrance. SAP confirms to ensure that Customer Personal Data is provided in a structured, commonly used, and machine-readable format as specified in the CSA. SAP also confirmed that Customer Personal Data is appropriately deleted within the agreed timescale.

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.

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

In accordance with sections 3.3.1.2 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: August 2024

Valid until: August 2025

Verification-ID: 2024LVL02SCOPE5421

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