SCOPE EUROPE

Verification of Declaration of Adherence

Declaring Company: SAP SE

Verification-ID	2021LVL02SCOPE319
Date of Approval	December 2021
Valid until	December 2022

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 being drafted by the Cloud Select Industry Group[3] (**'C-SIG'**) the EU Cloud CoC, at that time being called C-SIG Code of Conduct on data protection for Cloud Service Providers, the Code was developed against Directive 95/46/EC[4] incorporates 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 Cloud for Customer (C4C)

SAP Cloud for Customer with its two components SAP Sales Cloud and SAP Service Cloud facilitates sales and service people to engage with their customers by providing functionalities to close deals and provide support through collaboration and ticket tools which targets the different resources. By assigning tasks automatically to the right resource and providing the integration to different knowledge bases, a quicker and more efficient response to customer inquiries is possible. Part of C4Cs security functionalities are for example the customer's possibility to bring their own key for encryption, as well as setting their own deletion and retention time frames, enabling read access logging and limiting access through the definition of different roles and exporting stored personal data in case of data subject requests)[6]

SAP Cloud for Customer (C4C) has been declared adherent with its two components SAP Sales Cloud and SAP Service Cloud, where for each SAP takes responsibility for the Data Centres, Hardware and Infrastructure management, Customer System Administration Services, and Monitoring.

---

[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] **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.

2.1.1 SAP Sales Cloud[7]

SAP Sales Cloud provides Sales people with a robust set of capabilities to engage in meaningful customer conversations and deliver the right impact every time. Going beyond the traditional approach, SAP Sales Cloud provides delightful user experience and equips your sales team to close more deals faster in today's complex selling environment[8]

2.1.2 SAP Service Cloud[9]

With SAP Service Cloud, service agents have customer information at their fingertips. By using available collaboration tools and knowledge base they know which service resources are available to address a customer need immediately. Technicians can order spare parts, check inventory, manage tasks, and complete service jobs on their mobile devices.[10]

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[11].

3.1 Approval of the Code and Accreditation of the Monitoring Body

The services concerned passed the verification process by the Monitoring Body of the EU Cloud CoC, i.e., SCOPE Europe sprl/bvba[12].

The Code has been officially approved May 2021[13]. SCOPE Europe has been officially accredited as Monitoring Body May 2021[14]. 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.[15]

---

[7] https://www.sap.com/products/sales-cloud.html
[8] **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.
[9] https://www.sap.com/products/service-cloud.html
[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://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679
[12] https://scope-europe.eu
[13] https://www.gegevensbeschermingsautoriteit.be/publications/decision-n05-2021-of-20-may-2021.pdf
[14] https://www.gegevensbeschermingsautoriteit.be/publications/decision-n-06-2021-of-20-may-2021.pdf
[15] https://eucoc.cloud/en/public-register/assessment-procedure/

3.2 Principles of the Verification Process

Notwithstanding the powers of and requirements set-out by the supervisory authority pursuant 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; pro-actively 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 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 Control's Catalogue, to the Monitoring Body.

The CSP may do so either by referencing existing third-party audits or certifications and their respective reports or by free text. Additionally, the CSP will have to provide a general overview on the functionalities, technical and organizational and contractual frameworks of the service(s) declared adherent.

With regards to internationally recognized 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 request for further, detailed information including potentially confidential information. Within any other Recurring Assessment, the Monitoring Body will select an appropriate share of Controls provided both that over a due period every Control will be subject to scrutiny by the Monitoring Body and aspects of increased attention as indicated e.g., by media reports, publications and actions of supervisory authorities are covered.

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 indications for appropriate implementation by the Control Guidance, then the Monitoring Body verifies the service(s) declared adhered as compliant and thereupon make 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 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 recognized 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 recognized 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 up to 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[16] and refer to the Public Register of the EU Cloud CoC[17] to enable Customers to verify the validity of adherence.

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

4.1 Fact Finding

Following the declaration of adherence of SAP SE ('**SAP SE**'), the Monitoring Body provided SAP SE with a template, requesting SAP SE 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, and are embedded in the same contractual framework.

SAP SE elaborated the process to establish Customers' instances and the responsibilities of SAP SE being in scope, i.e., Data Centres, Hardware and Infrastructure management, Customer System Administration Services, and Monitoring. As SAP C4C enables Customers to independently integrate and deploy Cloud Applications fit for their needs, both the integration and deployment has been out of scope of this verification process because these do not represent responsibilities of the SAP SE as CSP under the Code.

SAP SE promptly responded to the template. 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 SE provided information illustrating the actual structure of the services declared adherent and describing the technical and contractual framework.

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[18], the Monitoring Body analysed the responses and information provided by SAP SE.

---

[16] https://eucoc.cloud/en/public-register/levels-of-compliance/
[17] https://eucoc.cloud/en/public-register/
[18] https://eucoc.cloud/en/about/about-eu-cloud-coc/applicable-procedures/

SAP SE declared services have been externally certified and audited, e.g., SAP SE holds current ISO 27001 and 27018 certificates. The declaration of adherence referred to the respective ISO certifications 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 indicate compliance.

4.3 Examined Controls and related findings by the Monitoring Body

4.3.1 Examined Controls

The Monitoring Body reviewed the initial submission from SAP SE which outlined how all the requirements of the Code were met by SAP SE 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.D, 5.1.E, 5.2.E, 5.3.E, 5.3.F, 5.3.G, 5.4.A, 5.6.A, 5.7.F, 5.8.B, 5.12.C, 5.14.C, 5.14.E, 6.1.C, 6.2.H, 6.2.I, 6.2.P.

4.3.2 Findings by the Monitoring Body

Monitoring Body verified that declared Cloud Services qualify both as Cloud Service under the Code and as Cloud Service Family. SAP SE provided information outlining the structure of the services, contractual and supporting documents enabling the Monitoring Body to better understand SAP SE's service offerings. The service offerings qualify as Cloud Service in the sense of the Code given the shared responsibility model. The Code explicitly does not limit Cloud Services to any kind of service offerings, i.e., Anything as a Service (XaaS) approach. Additionally, Monitoring Body assessed whether the provided references to the declared services are unambiguously clear to Customers. In scope of this declaration of adherence is the management and configuration platform. This report does not provide any indication whether any applications deployed by Customers via such platform will be compliant with the Code, neither does this report indicate any compliance of individual components that can be accessed via the declared Cloud Services. It is worth noting, though, that Customers may refer to the Public Register of the Code. Such components may, subject to a separate process, have been declared adherent to the Code by Cloud Service Providers, including by SAP SE.[19] Monitoring Body

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

also understands that declared Cloud Services qualify as Cloud Service Family, because SAP SE submitted documentation supporting the overarching technical and organisational, including contractual, framework.

Monitoring Body focussed on verifying existing mechanisms and procedures, including policies, ensuring SAP SE is meeting the requirements of the Code at the time of verification but will also hold up the level of proception provided by the Code at a minimum in future.

During the process of verification, SAP SE consistently gave impression of having prepared the Declaration of Adherence well and thoroughly. Responses being provided were detailed and never created any impression of intentional non-transparency. Requests for clarification or additional, supporting information and / or evidence were promptly dealt with and always met the deadlines set by the Monitoring Body. It is worth noting that SAP SE provided extensive responses, including both free text but also references as well as quotes and copies of relevant policies upfront. The provision of such underpinning documents and information eases the Monitoring Body's assessment as claims can verified easily without follow-up request. At the same time, Monitoring Body requested additional information, where appropriate, also to verify that provided underpinning information where accurate and current.

The Code requires that Cloud Service Providers transparently communicate applicable retention on Customer Personal Data, alternatively, enable Customers to manage retention of their respective Customer Personal Data individually and exhaustively. A review of provided information by SAP SE convincingly indicated that Customers are properly enabled to manage retention of their Customer Personal Data.

The latter coincides with Customers' possibilities to retrieve Customer Personal Data. SAP SE enables Customers to adequately retrieve their entrusted Customer Personal Data, both during the term of the Cloud Service Agreements and at the end of the service provisioning.

SAP SE provides Customers with the capability to determine the period upon which Customer Personal Data shall be deleted after termination of contract. SAP SE transparently communicates to Customers when Customer Personal Data will also be removed in existing back-ups.

Regarding encryption in transit and implementation of state-of-the-art techniques of encryption in general, SAP SE provided thorough information meeting the Code's requirements. SAP SE also interlinked security incident and data breach incident response mechanisms to ensure that any potential incident will be treated accordingly and in accordance with the Code's requirements.

Changes of subprocessors are communicated to Customers transparently via a dedicated platform, i.e., My Trust Center. Customers are informed about the possibility to subscribe to an email notification service. In case of changes, Customers are provided with adequate means to object such changes as provided by the Code. The list of subprocessors also enables Customers to identify applicable jurisdictions based on their locations.

In cases where Customers request additional information on GDPR related matters, including SAP SE's compliance, SAP SE provides support to Customers by several means. When sharing information with requesting Customers, SAP SE has implemented procedures ensuring that security and confidentiality of Customer Personal Data of other Customers is maintained.

5 Conclusion

Given answers by SAP SE were consistent. Where necessary SAP SE 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[20] alongside this report.

In accordance with sections 3.4.1.2 and 3.4.2 and given the type of information provided by SAP SE to support the compliance of its service, the Monitoring Body grants SAP SE 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[21].

Verification-date: December 2021 **Valid until**: December 2022

Verification-ID: 2021LVL02SCOPE319

[20] https://eucoc.cloud/en/public-register/
[21] https://eucoc.cloud/en/public-register/