SCOPE EUROPE

Verification of Declaration of Adherence

Declaring Company: SAP SE

Verification-ID	2021LVL02SCOPE319
Date of Approval	December 2022
Valid until	December 2023

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 – was developed against Directive 95/46/EC[4] and 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 to comply with GDPR requirements are for example protecting customer personal data through following communication encryption standards, the customer's possibility to define access roles that enable the customer to implement an information based authorization concept and control and limit access to personal data, as well as setting their own deletion and retention time frames, enabling read access logging 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 its own data centres, and hardware as well as 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]

2.2 SAP Commerce Cloud[11]

SAP Commerce Cloud enables customers to build their digital commerce solution in Business to B2B or B2C scenarios and delivers an engaging and profitable commerce experience by selling their products, solutions, and services. As e-commerce platform, SAP Commerce Cloud is not only PCI certified, it also protects the customer's personal data by following authentication mechanism standards or communication encryption.[12]

2.3 SAP Customer Data Solutions[13]

SAP's Customer Data Solutions connects information across the customer's enterprise to achieve business decision information, build trust and strengthen loyalty by connecting customer data with back-office data and create better customer views and respecting data privacy by operating permission-based data.[14]

---

[7] SAP Sales Cloud | Sales Automation Software for Enterprises and SMEs
[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] SAP Service Cloud: CRM Service Software for Enterprises and SMEs
[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/crm/e-commerce-platforms.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/crm/customer-data-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.

2.3.1 SAP Customer Data Cloud

SAP Customer Data cloud (CDC) is an identity management solution for B2B and B2C scenarios and a solution for consent and preference management. Customers of SAP CDC can configure data privacy related functionalities to be compliant with GDPR requirements. These cover for example deletion functionalities, change logs or download functions to retrieve personal data of a data subject[15]

2.3.2 SAP Customer Data Platform

SAP Customer Data Platform (CDP) supports customers in connecting end user data to deliver a better end user experience. Permission based customer data can be connected to further CRM and ERP solutions as SAP Cloud for Customer. SAP CDP provides data protection and privacy related functionalities to enable customers to configure deletion, extract personal data of a data subject or by logging changes to personal data.[16]

3 Verification Process - Background

V2.11 of the EU Cloud CoC has been developed against GDPR and hence provides mechanisms as required by Articles 40 and 41 GDPR[17].

3.1 Approval of the Code and Accreditation of the Monitoring Body

The services concerned passed the verification process by the Monitoring Body of the EU Cloud CoC, i.e., SCOPE Europe sprl/bvba[18].

The Code has been officially approved May 2021[19]. SCOPE Europe has been officially accredited as Monitoring Body May 2021[20]. The robust and complex procedures and mechanisms can be reviewed by any third party in detail at the website of the EU Cloud CoC alongside a short summary thereof.[21]

---

[15] **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.
[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.
[17] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679
[18] https://scope-europe.eu
[19] https://www.gegevensbeschermingsautoriteit.be/publications/decision-n05-2021-of-20-may-2021.pdf
[20] https://www.gegevensbeschermingsautoriteit.be/publications/decision-n-06-2021-of-20-may-2021.pdf
[21] https://eucoc.cloud/en/public-register/assessment-procedure/

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 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 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 organisational 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 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 indications for 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 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[22] and refer to the Public Register of the EU Cloud CoC[23] to enable Customers to verify the validity of adherence.

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

4.1 Fact Finding

Following the declaration of adherence of SAP SE ('**SAP**'), the Monitoring Body provided SAP with a template, requesting SAP to detail its compliance with each of the Controls of the EU Cloud CoC.

As this declaration is a renewal,[24] 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 and organisational and contractual framework as the original Cloud Services.

SAP 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 provided information illustrating the actual structure of the services declared adherent and describing the technical, organisational 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[25], the Monitoring Body analysed the responses and information provided by SAP.

---

[22] https://eucoc.cloud/en/public-register/levels-of-compliance/
[23] https://eucoc.cloud/en/public-register/
[24] You can access the Verification Report(s) of previous year(s) via the following link(s): Verification Report 2021
[25] https://eucoc.cloud/en/about/about-eu-cloud-coc/applicable-procedures/

SAP's declared services have been externally certified and audited. SAP holds an ISO 27001:2017 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 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, 5.2.B, 5.2.C, 5.3.C, 5.3.F, 5.4.A, 5.5.A, 5.5.B, 5.5.E, 5.7.A, 5.7.B, 5.7.C, 5.8.A, 5.9.B, 5.10.B, 5.11.B, 5.11.C, 5.12.C, 5.13.A, 5.14.A, 5.14.B and 5.14.F.

4.3.2 Findings by the Monitoring Body

The Monitoring Body would like to highlight that the renewal has been triggered in due time by SAP. Responses were provided in accordance with requested deadlines. The Monitoring Body was never of the impression that SAP was not acting in compliance with the Code.

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 and organisational 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 paid attention to appropriate procedures and sufficient enablement of Customers. One field of assessment has been the procedures for addressing individual Customer inquiries,

complaints and disputes around non-compliance to the Code. Customers are provided with the possibility to do so via internal tools provided by SAP, regardless of the possibility to file complaints directly to the Monitoring Body.

The Monitoring Body assessed SAP's mechanisms for the transfer of personal data to third countries. SAP uses Standard Contractual Clauses (SCCs) as a safeguard for such transfers.

The procedures related to Customers' Audit Rights were assessed. The assessment focused on SAP's methodology to determine the costs of audits, as well as the possibility for Customers to request additional evidence of compliance. SAP provided the Monitoring Body with an overview of the methodology to determine the costs of audits. As indicated by SAP, Customers are also provided with the relevant communication channels to request additional evidence of compliance, without necessarily exercising its audit rights.

SAP's records of processing activities ('ROPA') built another area of focus. Based on the information provided, SAP maintains a ROPA in its capacity as Processor, which includes the relevant information as per Article 30.2 GDPR. In addition to this, the relevant communication channels for Customers providing the relevant information in relation to the completion and relevancy of the ROPA, as well as changes in subprocessors and Customers accessing relevant information to comply with their obligations and duties under the GDPR were confirmed by SAP.

The Code requires CSPs to assist Customers to respond to data subject requests. SAP provides Customers with self-service functionalities to enable them to respond to data subject requests, given the responses by SAP. Likewise, where Customers may require additional support, SAP also offers different channels to support Customers in this respect.

Finally, the Monitoring Body assessed SAP's data deletion policies, acknowledging that SAP Cloud Services are instantiated by means of Virtual Machines. Based upon SAP's documentation, SAP implements tenant decommissioning and deactivation of Customer's account, as well as sanitising Customer Personal Data, including means to multiple rewriting respectively overwriting or by purging such data.

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 services will be listed in the Public Register of the EU Cloud CoC[26] 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 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 CoC[27].

Verification-date: December 2022 **Valid until**: December 2023

Verification-ID: 2021LVL02SCOPE319

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