SCOPE EUROPE

Verification of Declaration of Adherence | Renewal June 2021

Declaring Company: SAP SE

EU CLOUD COC

Verification-ID	2021LVL02SCOPE216
Date of Approval	June 2021
Valid until	June 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.This verification has been successfully completed as indicated in the Public Verification Report[3] as of June 2021 following this renewal.

Originally being drafted by the Cloud Select Industry Group[4] (**'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[5] 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'**)[6].

2 List of declared services

2.1 SAP Business Technology Platform[7]

SAP Business Technology Platform (SAP BTP) is a Platform as a Service ("PaaS") offering for the Intelligent Enterprise. Customers can achieve agility, business value, and continual innovation through integration, data to value, and extensibility of all SAP SE and third-party applications and data assets based on strong data protection and privacy principles.[8]

The Cloud Service Family (SAP BTP) comprises of the following Cloud Services

Application Autoscaler Service
Business Entity Recognition
Data Attribute Recommendation
Document Classification
Document Information Extraction
Hyperledger Fabric on SAP BTP
Identity and Authentication
Identity Provisioning
Invoice Object Recommendation
Java Application Lifecycle Management for SAP BTP
Java Debugging for SAP BTP

[1] https://eucoc.cloud
[2] https://eucoc.cloud/get-the-code
[3] Download and access reports of prior assessments: Verification Report 2021
[4] https://ec.europa.eu/digital-single-market/en/cloud-select-industry-group-code-conduct
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046
[6] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679
[7] SAP Business Technology Platform
[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.

Java Profiling for SAP BTP
MongoDB on SAP BTP
MultiChain on SAP BTP
OAuth 2.0 on SAP BTP
Object Store on SAP BTP
PostgreSQL on SAP BTP
PostgreSQL on SAP BTP, hyperscaler option
RabbitMQ on SAP BTP
Redis on SAP BTP
Redis on BTP, hyperscaler option
SAP Alert Notification service for SAP BTP
SAP Analytics Cloud including SAP Digital Boardroom and SAP Analytics Hub
SAP Application Logging Service for SAP BTP
SAP ASE service
SAP Audit Log service
SAP Authorization and Trust Management service
SAP BTP, ABAP environment
SAP BTP, Cloud Foundry runtime
SAP BTP, Kyma runtime
SAP BTP, Neo runtime
SAP BTP, Serverless runtime
SAP Business Application Studio
SAP Cloud for Energy
SAP Cloud Identity Access Governance
SAP Cloud Integration for data services
SAP Cloud Portal service
SAP Cloud Transport Management
SAP Connectivity service
SAP Continuous Integration and Delivery
SAP Credential Store
SAP Custom Domain service
SAP Data Privacy Integration
SAP Data Quality Management
SAP Data Retention Manager
SAP Data Warehouse Cloud
SAP Destination service
SAP Digital Manufacturing Cloud
SAP Document Center
SAP Document Management service (incl. integration option, application option)
SAP Document service
SAP Edge Services
SAP Event Mesh
SAP Feature Flags service
SAP Fiori Cloud
SAP Fiori Mobile
SAP Forms service by Adobe
SAP Git service
SAP HANA Cloud (incl. SAP HANA database and SAP HANA Cloud, data lake)
SAP HANA service for SAP BTP
SAP HANA Spatial Services
SAP HTML5 Application Repository service for SAP BTP
SAP Information Collaboration Hub
SAP Integration Suite (incl. SAP API Management, Cloud Integration, Integration Advisor, Open Connectors)
SAP Intelligent Robotic Process Automation
SAP Internet of Things
SAP Job Scheduling service
SAP Keystore service
SAP Kubernetes Gardener (internal consumption only)
SAP Launchpad service
SAP Leonardo Machine Learning Foundation

SAP Logistics Business Network (incl. freight collaboration option, global track and trace option, material traceability option)
SAP Market Rates Management (incl. bring your own rates, refinitive data option)
SAP Mobile services
SAP Monitoring service for SAP BTP
SAP OData Provisioning
SAP Platform Identity Provider service for SAP BTP
SAP Software-as-a-Service Provisioning service
SAP Solutions Lifecycle Management service for SAP BTP
SAP Sports One
SAP Subscription Billing
SAP Virtual Machine service
SAP Web Analytics
SAP Web IDE
SAP Workflow Management (incl. Workflow Service, SAP Business Rules, SAP Process Visibility service)
Service Ticket Intelligence
UI Theme Designer
UI5 flexibility for key users

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[9].

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[10].

The Code has been officially approved May 2021. SCOPE Europe has been officially accredited as Monitoring Body May 2021. 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.[11]

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

[9] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679
[10] https://scope-europe.eu
[11] https://eucoc.cloud/en/public-register/assessment-procedure/

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.

4 Transparency about adherence

Each service adherent to the EU Cloud CoC must transparently communicate its adherence by both using the appropriate Compliance Mark[12] and refer to the Public Register of the EU Cloud CoC[13] to enable Customers to verify the validity of adherence.

5 Subject of this Renewal Assessment

Due to internal renaming, SAP SE renewed the Declaration of Adherence early, to update the naming and branding of listed Cloud Services. Originally the Cloud Services Family was referred to as *SAP Cloud Platform* which shall be referred to as *SAP Business Technology Platform*. SAP SE confirmed, that no updates regarding relevant matter of the Code took place, but this update only related to the branding of the Cloud Services.

Additionally, SAP SE has renewed its ISO/IEC 27001 certificate. The updated scope of the ISO/IEC 27001 certificate aligns with the original scope of the Initial Assessment[14]. Back then SAP SE confirmed to align the declared Cloud Service and the certificate's scope according to the certificate's renewal cycle. Whilst those services were in scope of the Initial Assessment, their publication was requested by SAP SE to be postponed until the certificates will be updated.

Furthermore, five additional Cloud Services also coming along with the renewal of SAP SE's Declaration of Adherence. Considering the provided information on the technical and contractual infrastructure that is being shared within all declared Cloud Services as well as the convincing answers and references, including an explicit confirmation that there is no material difference, provided by SAP SE in the Initial Assessment, Monitoring Body has no reason to either doubt that the additional services do not meet the expected requirements nor that the services are not part of the same service family, especially as they existing third-party validation assessed them jointly, as well.

6 Conclusion

This Renewal was only intended to update the Cloud Services brand names and aligning SAP SE's renewal cycles of ISO/IEC 27001 EU Cloud CoC. The minor addition of Cloud Services was reasoned by SAP SE. Monitoring Body did not perform an additional in-depth assessment for this renewal-statement, as between the Initial Assessment and the early renewal request by SAP SE was less than one

[12] https://eucoc.cloud/en/public-register/levels-of-compliance/
[13] https://eucoc.cloud/en/public-register/
[14] Download and access reports of prior assessments: Verification Report 2021

month. Therefore, the Monitoring Body verifies all services as compliant with the EU Cloud CoC. In addition to the original public report[15] the services will be listed in the Public Register of the EU Cloud CoC[16] alongside this report.

7 Validity

This renewal report comprises of 10 pages. It is valid until the next official renewal of the upgraded Declaration of Adherence. This upgrade statement has been attached to the original Verification Report that follows this statement.

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

Verification-ID: 2021LVL02SCOPE216

[15] Download and access reports of prior assessments: Verification Report 2021
[16] https://eucoc.cloud/en/public-register/

SCOPE EUROPE

Verification of Declaration of Adherence

Declaring Company: SAP SE

Verification-ID	2021LVL02SCOPE216
Date of Approval	June 2021
Valid until	June 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 Business Technology Platform

SAP Business Technology Platform (SAP BTP) is a Platform as a Service ("PaaS") offering for the Intelligent Enterprise. Customers can achieve agility, business value, and continual innovation through integration, data to value, and extensibility of all SAP and third-party applications and data assets based on strong data protection and privacy principles.[6]

The Cloud Service Family comprises of following Cloud Services[7]

Application Autoscaler Service
Business Entity Recognition
Data Attribute Recommendation
Document Classification
Document Information Extraction
Hyperledger Fabric on SAP BTP
Identity and Authentication
Identity Provisioning
Invoice Object Recommendation
Java Application Lifecycle Management for SAP BTP
Java Debugging for SAP BTP
Java Profiling for SAP BTP
MongoDB on SAP BTP
MultiChain on SAP BTP
OAuth 2.0 on SAP BTP

[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.
[7] Amended in accordance with the Renewal Statement above; Download and access the original reports of prior assessments: Verification Report 2021

Object Store on SAP BTP
PostgreSQL on SAP BTP
PostgreSQL on SAP BTP, hyperscaler option
RabbitMQ on SAP BTP
Redis on SAP BTP
Redis on BTP, hyperscaler option
SAP Alert Notification service for SAP BTP
SAP Analytics Cloud including SAP Digital Boardroom and SAP Analytics Hub
SAP Application Logging Service for SAP BTP
SAP ASE service
SAP Audit Log service
SAP Authorization and Trust Management service
SAP BTP, ABAP environment
SAP BTP, Cloud Foundry runtime
SAP BTP, Kyma runtime
SAP BTP, Neo runtime
SAP BTP, Serverless runtime
SAP Business Application Studio
SAP Cloud for Energy
SAP Cloud Identity Access Governance
SAP Cloud Integration for data services
SAP Cloud Portal service
SAP Cloud Transport Management
SAP Connectivity service
SAP Continuous Integration and Delivery
SAP Credential Store
SAP Custom Domain service
SAP Data Privacy Integration
SAP Data Quality Management
SAP Data Retention Manager
SAP Data Warehouse Cloud
SAP Destination service
SAP Digital Manufacturing Cloud
SAP Document Center
SAP Document Management service (incl. integration option, application option)
SAP Document service
SAP Edge Services
SAP Event Mesh
SAP Feature Flags service
SAP Fiori Cloud
SAP Fiori Mobile
SAP Forms service by Adobe
SAP Git service
SAP HANA Cloud (incl. SAP HANA database and SAP HANA Cloud, data lake)
SAP HANA service for SAP BTP
SAP HANA Spatial Services
SAP HTML5 Application Repository service for SAP BTP
SAP Information Collaboration Hub
SAP Integration Suite (incl. SAP API Management, Cloud Integration, Integration Advisor, Open Connectors)
SAP Intelligent Robotic Process Automation
SAP Internet of Things
SAP Job Scheduling service
SAP Keystore service
SAP Kubernetes Gardener (internal consumption only)
SAP Launchpad service
SAP Leonardo Machine Learning Foundation
SAP Logistics Business Network (incl. freight collaboration option, global track and trace option, material traceability option)
SAP Market Rates Management (incl. bring your own rates, refinitive data option)
SAP Mobile services

SAP Monitoring service for SAP BTP
SAP OData Provisioning
SAP Platform Identity Provider service for SAP BTP
SAP Software-as-a-Service Provisioning service
SAP Solutions Lifecycle Management service for SAP BTP
SAP Sports One
SAP Subscription Billing
SAP Virtual Machine service
SAP Web Analytics
SAP Web IDE
SAP Workflow Management (incl. Workflow Service, SAP Business Rules, SAP Process Visibility service)
Service Ticket Intelligence
UI Theme Designer
UI5 flexibility for key users

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[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 sprl/bvba[9].

The Code has been officially approved May 2021. SCOPE Europe has been officially accredited as Monitoring Body May 2021. 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.[10]

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

[8] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679
[9] https://scope-europe.eu
[10] https://eucoc.cloud/en/public-register/assessment-procedure/

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[11] and refer to the Public Register of the EU Cloud CoC[12] 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 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[13], the Monitoring Body analysed the responses and information provided by SAP SE.

SAP SE declared services have been externally certified and audited, e.g., SAP SE holds current SOC 2, ISO 27001 and 27017 and C5 certificates. 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 did verify the certification and references. Current certifications – individually – were not covering the full spectrum of declared cloud service. Upon request, SAP SE convincingly explained this is subject to an ongoing restructure of the cloud services and, thus, related certificates

[11] https://eucoc.cloud/en/public-register/levels-of-compliance/
[12] https://eucoc.cloud/en/public-register/
[13] https://eucoc.cloud/en/about/about-eu-cloud-coc/applicable-procedures/

and audit reports. SAP SE stated that upcoming renewals of such certificates and audits will extend their scope accordingly. Considering the provided explanations on the technical and contractual infrastructure that is being shared within all declared Cloud Services, Monitoring Body has no reason to a) doubt that non-covered services are not, yet, subject to the same measures as indicated and verified by current certificates and b) that SAP SE will align their scoping with each renewal of the applicable certificates and audit reports. 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, 5.4.B, 5.4.E, 5.5.B, 5.5.E, 5.5.F, 5.7.D, 5.8.A, 5.12.A, 5.14.C, 5.14.D, 5.14.E, 6.1.C, 6.2.H, 6.2.I, 6.2.P.

4.3.2 Findings by the Monitoring Body

The Monitoring Body verified that submitted Cloud Services qualify as Cloud Service Family. SAP SE provided a dossier outlining the technical architecture. Alongside, SAP SE provided contractual documents and Customer supporting information. Information convincingly indicated that declared Cloud Services qualify as a Cloud Service Family.

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.

On area where the Monitoring Body requested further information has been sub-processor's management. SAP SE implemented a sub-processors onboarding programme. Mechanisms to flow-down SAP SE's obligations throughout the sub-processor chain as well as the due onboarding and recurring scrutiny of sub-processors have been of interest. SAP SE convincingly described its process, consisting of different means, such as questionnaires, interviews, SAP performed audits and analysis of existing third-party certificates and audits. The diverse and active measures meet the requirements of the Code.

Another area of interest has been the change of applicable jurisdictions. SAP SE, in general, provides its services word-wide, i.e., by principle, Customers accept and authorize third-country transfer provided those will be subject to appropriate safeguards. Customers have access to a current list of applicable third countries, acknowledging that such list may change from time to time without any impact on the service provision. Additionally, Customers are offered a dedicated so-called "EU Access" only option. Upon active and distinct choice of Customer, SAP SE will provide its services without any third-country transfers.

Given the multitude of Cloud Services subject to this Declaration of Adherence, minor differences are expected and in accordance with the Code requirements. Such differences were indicated by SAP SE, e.g., regarding the possibilities to export Customer Personal Data in a machine readable, commonly used, structured format. To verify that Customers are provided with sufficient means to identify existing possibilities and such possibilities meet the requirements of the Code, SAP SE was requested to provide samples of such communication. All samples provided were compliant with the Code.

Clarification was kindly requested related the period after which Customer Personal Data will be ultimately and irrevocably deleted respectively destroyed ("deleted"). Customer is provided with a grace period of 60 days, after which Customer Personal Data will be deleted including any applicable backups.

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.

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[14] 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 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[15].

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

Verification-ID: 2021LVL02SCOPE216

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