SCOPE EUROPE

Verification of Declaration of Adherence

Declaring Company: TEMENOS CLOUD SWITZERLAND SA

Verification-ID	2023LVL02SCOPE5317
Date of Approval	January 2024
Valid until	January 2025

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 drafted by the Cloud Select Industry Group[3] (**'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/EC[4] 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

Temenos offers cloud-native, cloud-agnostic front office and core banking, payments, fund management and wealth management software products enabling banks to deliver consistent, frictionless customer journeys and gain operational excellence.[6]

2.1 Temenos Transact[7]

Temenos Transact is the market leading core banking product which incorporates the broadest and deepest set of functionalities available in the market. The product is further enriched by an extensive set of Country Model Banks. Temenos Transact exploits new technologies to facilitate ease of use and ubiquity of access of everyday products and services for the end customer and enabling banks to meet their customers ever increasing expectations. A capable product factory provides support across all product lines, and is supported by an extensive set of embedded analytics which helps to give immediate customer insight and also vital support when designing new products or looking at financial and operational performance in context.[8]

- Accounts
- Cash Management

---

[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] https://www.temenos.com/products/core-banking/corporate-bank
[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.

- Customer output
- Deposits
- Lending
- Treasury

2.2 Temenos Infinity

Temenos Infinity is an independent digital banking product built on a market leading multi experience digital platform. It focuses on customer engagement and the distribution of banking products and services on an omni-channel basis.[9]

- Corporate Lending Origination System (CLOS) [10]
- SME Journey[11]

2.3 Temenos Payments[12]

Temenos Payments cover the complete payments lifecycle from order intake to clearing and settlement. These solutions are designed to work successfully both separately or together, via SaaS, cloud, or on-premise, providing the flexibility to tailor payment solutions to suit simple, complex and diverse needs. Temenos Payments solution includes Payments Hub (TPH), ISO20022 payment repair, Payment Order Management, Request to Pay, Payments SaaS, Instant Payments, Swift GPI or Embedded Analytics. [13]

- Payment Orders
- Payments

2.4 Regulatory Compliance[14]

Regulatory Compliance provides solution to assists clients to identify and process personal data in accordance with data protection, helps Foreign Financial Institutions (FFIs) to comply with legislations. Financial Risk management solutions have the ability to comply with complex risk and regulatory requirements and run sophisticated risk analytical models.[15]

- Customer Tax Regulation

---

[9] **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.
[10] https://www.temenos.com/products/digital-banking/temenos-infinity-consumer-loan-origination/
[11] https://www.temenos.com/products/digital-banking/temenos-infinity-journey-manager/
[12] https://www.temenos.com/products/payments/
[13] **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.
[14] https://www.temenos.com/products/regulatory-compliance/
[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.

- Financial Risk Management
- Data Protection and Consent

2.5 Temenos Wealth Suite[16]

Temenos Wealth provides an integrated portfolio management and securities trading platform for wealth managers and private bankers. It is also pre-integrated into Temenos Infinity to provide a seamless front-to-back wealth solution that is applicable in any type and size of bank or wealth manager, across multiple entities and geographies, across all customer markets, via multiple innovative channels, consistently and in real-time, on-premise or cloud.[17]

- WSFO - Channels

2.6 Temenos Financial Crime Mitigation[18]

Temenos Financial Crime Mitigation provides with a single product family incorporating Sanctions Screening, PEP Matching, KYC risk scoring and categorization, AML Transaction Monitoring and fraud mitigation, and support all user functions including alert management, case management, reporting and dashboards.[19]

- Financial Crime Mitigation

2.7 Temenos Analytics[20]

Temenos Analytics is a comprehensive Reporting, Analytics and Business Intelligence product allowing banks to be more efficient and profitable by providing robust, banking specific, financial, profitability, customer, and digital analytics.[21]

- Analytics

---

[16] https://www.temenos.com/solutions/wealth-management-private-banking/temenos-wealth-front-office/
[17] **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.
[18] https://www.temenos.com/products/financial-crime-mitigation/
[19] **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.
[20] https://www.temenos.com/products/data-and-analytics/
[21] **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.

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[22].

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[23].

The Code has been officially approved in May 2021[24]. SCOPE Europe has been officially accredited as Monitoring Body in May 2021[25]. 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.[26]

3.2 Principles of the Verification Process

Notwithstanding the powers of and requirements set out by the supervisory authority pursuant to Article 41 GDPR, the Monitoring Body will assess whether a Cloud Service, 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.

3.3 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

[22] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679
[23] https://scope-europe.eu
[24] https://www.gegevensbeschermingsautoriteit.be/publications/decision-n05-2021-of-20-may-2021.pdf
[25] https://www.gegevensbeschermingsautoriteit.be/publications/decision-n-06-2021-of-20-may-2021.pdf
[26] 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.

3.4 Process in Detail

It is expected that, prior to any assessment of the Monitoring Body, each CSP assesses its compliance internally. When declaring its service(s) adherent to the EU Cloud CoC, each CSP must elaborate its compliance with each of the Controls as provided by the Code considering the Control Guidance, as provided by the Controls Catalogue, to the Monitoring Body.

The CSP may do so either by referencing existing third-party audits or certifications, their respective reports and by free text responses. Additionally, the CSP will have to provide a general overview of the functionalities, technical, 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.

3.4.1 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 recognised by the Monitoring Body in the verification process concerned, are not covering an adequate share of Controls of this Code; such adequate share shall be subject to the discretion of the Monitoring Body, considering e.g., the share related to the overall amount of Controls of the Code or whether a full Section or topic is being covered.

3.4.1.3 Third Level of Compliance

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.

3.4.2 Final decision on the applicable Level of Compliance

When declaring its Cloud Service adherent, the CSP indicates the Level of Compliance it is seeking to achieve. Any final decision, whether a CSP is meeting the requirements of a specific Level of Compliance is at the sole discretion of the Monitoring Body.

3.5 Transparency about adherence

Each service adherent to the EU Cloud CoC must transparently communicate its adherence by both using the appropriate Compliance Mark[27] and referring to the Public Register of the EU Cloud CoC[28] to enable Customers to verify the validity of adherence.

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

4.1 Fact Finding

Following the declaration of adherence of TEMENOS CLOUD SWITZERLAND SA ('**Temenos**'), the Monitoring Body provided Temenos with a template, requesting Temenos 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

[27] https://eucoc.cloud/en/public-register/levels-of-compliance/
[28] https://eucoc.cloud/en/public-register/

hardware and software (i.e., technical framework), and are embedded in the same organisational and contractual framework.

Temenos 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. Temenos 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[29], the Monitoring Body analysed the responses and information provided by Temenos.

Temenos's declared services have been externally certified and audited. Temenos holds SOC 2 report and ISO 27001/27017/27018 certificates, 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.

4.3 Examined Controls and related findings by the Monitoring Body

4.3.1 Examined Controls

The Monitoring Body reviewed the submission from Temenos which outlined how all the requirements of the Code were met by Temenos's implemented measures. In line with the Monitoring Body's process outlined in Section 3.4, the Monitoring Body selected a subset of Controls from the Code for in-depth scrutiny. In-depth scrutiny reflects sample taking and follow-up questions, whilst the latter may address requests for clarifications or more detailed information. The Controls selected for this level of review were: 5.1.A, 5.1.F, 5.2.A, 5.2.E-G, 5.3.A-E, 5.4.A, 5.4.C, 5.4.E, 5.5.E, 5.7.A, 5.7.B, 5.7.D-F, 5.8.B, 5.10.A, 5.10.B, 5.11.A, 5.11.B, 5.12.C, 5.12.F, 5.12.G, 5.14.A, 5.14.C, 5.14.D, 5.14.F, 6.1.C, 6.2.P.

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

4.3.2 Findings by the Monitoring Body

During the process of verification, Temenos consistently prepared the Declaration of Adherence well and thoroughly. Temenos'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.

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 4.1), Temenos provided information outlining the structure of the services, contractual and supporting documents enabling the Monitoring Body to better understand Temenos's service offerings. Temenos provided explicit confirmation that all Cloud Services declared adherent belong to the same Cloud Service Family.

The Monitoring Body has focused on the subprocessor management program. Temenos has indicated that its SaaS Services are provided via Public Cloud Providers (currently Azure and AWS, which act as subprocessors), and that - apart from the Public Cloud Providers - currently Temenos' Affiliates are also used as subprocessors (and Customers agree that Temenos' Affiliates may be retained as subprocessors). As provided towards the Monitoring Body Temenos makes available a list of the subprocessors/Affiliates with relevant general information. In this regard, Temenos has in place a mechanism to notify the Customers about new subprocessors and provides the right to object. The timelines as well as the means to do so were confirmed by Temenos contractual documents. However, to the extent third-party subprocessors will be involved, the flow-down mechanisms are implemented to ensure that contractual obligations of subprocessors to adhere to the same standards of data processing as the Temenos are in place.

Further, the Monitoring Body has focused on the assistance provided to the Customers. Temenos makes available various communication channels for the Customers including public-facing website, Ticketing system, Customer Support Portal, and dedicated support email. Customers may receive support and request access or retrieve personal data by contacting Temenos via dedicated communication channels. In this vein, requested data is provided in industry standard formats. Along with it, Temenos has confirmed to have internal procedures to assist Customers with the Data Protection Impact Assessment (DPIA). Information Classification Policy is in place to ensure that no information provided to Customer in assistance of Customer's DPIA create a security risk themselves.

The Code requires CSPs to assist Customers to respond to data subject requests. In this regard Temenos indicated that data subject requests will not be processed, and the Customer would be notified

directly via Ticketing System. Additional assistance in obtaining relevant information to fulfil the data subject request would be provided to the Customer, if needed.

Temenos' records of processing activities ('ROPA') built another area of focus. Based on the information provided, the Monitoring Body was able to verify that Temenos maintains a ROPA in its capacity as Processor, which includes the relevant information as per Article 30.2 GDPR. The relevant communication channels for Customers to provide the information in relation to the completion and relevancy of the ROPA were confirmed by Temenos. Furthermore, Temenos conducts service review sessions on a regular basis and remains accessible to Customers via dedicated communication channels.

To the extent Customer Audit Rights are concerned, Temenos at the pre-contract signing stage makes available to the Customers upon-request relevant third-party certifications and reports. Most recent certificates, attestations and reports are made available to the Customers via Customer Support Portal. Further, Customers are enabled to request individual audits and Customer Audit Rights are included as standard part of the contractual agreements with Customers. In addition to this, Temenos provided the Monitoring Body with an overview of the approach to determine the costs of an audit.

Requests by supervisory authorities has also been in the scope of the assessment. Temenos confirmed its contractual obligations to provide assistance to the Customer to respond to requests by supervisory authorities and to provide relevant notification of such requests, as provided by the EU Cloud CoC. In addition to this, Temenos referred to an internal procedure operationalising requests received from regulators, including requests from supervisory authorities, which includes the steps taken by Temenos to deal with the respective requests internally and any potential internal escalations, as well as actions.

The provided information by Temenos also indicated that confidentiality obligations are in place with employees and contractors, which continue after the end of the respective agreements. Internal procedures are put in place to ensure that personnel are aware of their confidentiality obligations. In this regard, Temenos ensures security and privacy trainings for all its employees, at onboarding and annually thereafter. Additional training is also conducted specifically for the employees working with Customer Personal Data.

Another area of the assessment has been third country transfers. Temenos has confirmed that it relies on the adequacy decisions and has implemented safeguards as provided by Chapter V GDPR, as it implements the Standard Contractual Clauses (SCCs). Moreover, Temenos has confirmed to have

dedicated personnel that is responsible for the monitoring of the data privacy and protection compliance matters within Temenos Group and controlling whether the destination of a data transfer under the Cloud Service Agreement is subject to an adequacy decision of the European Commission.

5 Conclusion

The information provided by Temenos were consistent. Where necessary, Temenos 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[30] alongside this report.

In accordance with sections 3.4.1.2 and 3.4.2 and given the type of information provided by Temenos to support the compliance of its service, the Monitoring Body grants Temenos with a Second Level of Compliance.

6 Validity

This verification is valid for one year. The full report consists of 13 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[31].

Verification-date: January 2024 **Valid until**: January 2025

Verification-ID: 2023LVL02SCOPE5317

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