Verification of Declaration of Adherence

Declaring Company: TEMENOS CLOUD SWITZERLAND SA

Verification-ID	2023LVL02SCOPE5317
Date of Approval	January 2026
Valid until	January 2027

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' or 'Code')**[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 (**'CSPs'**) – 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

2.1 Temenos Core Banking[6]

Temenos Core, the core banking product of Temenos (formerly known as Transact), provides progressive core modernization capabilities and integrated solutions. It offers a l broad range of modular core banking capabilities, available in all market segments, such as Retail, Business, Corporate Banking, Wealth and Payments. With this modularity, and direct access to tooling on the platform, Temenos enables its Clients to adopt an incremental approach to modernization of their existing core banking technology and deliver innovative banking services at the forefront of their markets. Temenos Core is also supported by an extensive set of Country Model Banks. It also exploits new technologies to facilitate ease of use and ubiquity of access to everyday products and services for the end customer, enabling the banks to meet their customers' expectations. A capable product factory provides support across all product lines, and is supported by an extensive set of financial risk analytics, which provides customer insight and supports financial and operational performance.[7]

- Accounts
- Cash Management
- Customer output
- Deposits

---

[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] https://www.temenos.com/products/core-banking/
[7] **NOTE**: The content for the service description has been provided by the CSP and does not reflect any opinion of or assessment by the Monitoring Body.

- Lending
- Treasury
- Financial Risk Management

2.2 Temenos Digital[8]

Temenos Digital (formerly known as Infinity) is an independent digital banking product built on a digital platform that removes complexity and spans the end-to-end customer lifecycle from onboarding and account opening through to the servicing of these accounts.

Temenos Digital focuses on reimagining customer engagement by creating consistent experiences across various segments, such as Retail, Small Business, Corporate Banking and Wealth.

Temenos Journey Manager for customer acquisition and onboarding is a platform for building, managing and continuously improving onboarding journeys for all types of products. It comprises of multiple modules and tools that target different phases of the implementation process and provide capabilities for creating data collection forms, integrating third-party extensions like eSignatures, deployment and management of forms and the associated data, workflows, data delivery and optimization.[9]

- Journey Manager

2.3 Temenos Payments[10]

Temenos Payments covers the complete payments lifecycle from order intake to clearing and settlement. Temenos Payments is a payments processing platform that enables Temenos Clients/Banks or Payment Service Providers (PSPs) to modernize their capabilities to support continuous sustainable innovation in payments. The cloud native cloud agnostic, API-first architecture provides a modular environment suitable for operations of varying size and complexity, supporting retail, business, and corporate payment markets.[11]

Designed and built to support all payment types within a single, accessible hub, the open architecture supports the rapid onboarding of payment orders. Automated validations and enrichments help to

[8] https://www.temenos.com/products/digital-banking/
https://www.temenos.com/products/digital-banking/temenos-digital-journey-manager/
[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/payments/
[11] **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.

ensure STP rates as each payment flows through the configurable orchestration workflow with an optimized processing environment that is built on scalable, resilient technology.

The solutions offered by Temenos are compatible with any core banking, fraud and screening solution Model bank approach with configurations and are designed to operate on SaaS, cloud, or on-premises, providing the flexibility to tailor payment solutions to suit simple, complex and diverse needs. Temenos Payments solution includes among others Payments Hub (TPH), ISO 20022 Payment Repair Standards, formats, Payment Initiation and Payment Order Management, Request to Pay, Instant Payments, International Payments / Swift and Embedded Analytics.[12]

- Payment Orders
- Payments

2.4 Temenos Wealth[13]

Temenos Wealth is a wealth management solution that enables differentiation through superior digital and front-office capabilities. It delivers cost reductions with core automation, leverages the latest technology, and supports Temenos Clients with their end-to-end digital transformation and a composable front-to-back architecture. Wealth consists of standalone components that deliver an integrated, omnichannel solution to wealth managers and private bankers. It covers digital banking, customer relationship management, portfolio management, backoffice processing and market data management.

Temenos Wealth provides pre-integrated third-party solutions and digital solutions that enable self-service investing and hybrid advisory that is applicable in any type and size of bank or wealth manager, across multiple entities and geographies and across all markets, through multiple channels, consistently and in real-time, on-premise or cloud.[14]

- Digital Wealth
- Wealth Channels
- Data Source

[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.temenos.com/products/wealth-management/
[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.

2.5 Temenos Financial Crime Mitigation[15]

Temenos Financial Crime Mitigation is a single product family incorporating Sanctions Screening, PEP Matching, KYC risk scoring and categorization, AML Transaction Monitoring, fraud mitigation, and support all user functions including alert management, case management, reporting and dash-boards.

Temenos Financial Crime Mitigation (FCM) provides Temenos' Clients with flexibility to support all above user functions and helps reduce incorrect false positives in sanctions screening detection, AML Transaction Monitoring and payment fraud mitigation. FCM focus on the business problem of financial crime and compliance, addressing global regulatory challenges and offering flexibility, allowing Clients to choose from private or public cloud, On-premise or to be consumed as a fully managed service (SaaS).[16]

- Financial Crime Mitigation

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 SRL[18].

The Code has been officially approved in May 2021[19]. SCOPE Europe has been officially accredited as Monitoring Body in 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 https://www.temenos.com/products/financial-crime-mitigation/
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 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 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[22] and referring 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 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.

As this declaration is a renewal[24], the Monitoring Body requested from Temenos a confirmation that there has been no material change to the applicable technical and organisational and contractual framework. The Monitoring Body also requested from Temenos 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, organisational and contractual framework as the original Cloud Services.

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. This information was completed by the confirmations requested by the Monitoring Body as well as a detailed comparison of the declared Cloud Services between last year and this year verification highlighting the changes and the reasons for them.

---

[22] https://eucoc.cloud/en/public-register/levels-of-compliance/
[23] https://eucoc.cloud/en/public-register/
[24] You can access the Verification Report of previous year via the following link: Temenos - Verification Report – (2025)

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 Temenos.

Temenos's declared services have been externally certified and audited. Temenos maintains a SOC 2 report and ISO/IEC 27001:2022, 27017:2015, and 27018:2019 certificates, which are 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 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.C, 5.1.D, 5.1.E, 5.1.G, 5.3.C, 5.4.B, 5.4.C, 5.4.E, 5.4.F, 5.5.B, 5.5.C, 5.5.E, 5.7.A, 5.7.B, 5.8.A, 5.10.A, 5.10.B, 5.11.A, 5.12.A, 5.12.B, 5.12.D, 5.13.A, 5.13.B, 6.1.C, 6.1.D, and 6.2.I.

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.

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

Related to the Monitoring Body's requests (see section 4.1), Temenos indicated that no relevant changes to the Cloud Service Family were applied in regards of the implemented technical, organisational and contractual framework. Where additional Cloud Services were added, Temenos provided explicit confirmation that such Cloud Services belong to the same Cloud Service Family.

Temenos indicated that a Cloud Service Agreement (CSA) is in place with Customers determining the responsibilities of the Customers and the CSP regarding the security measures and the terms under which the Customer Personal Data shall be processed. Additionally, Temenos indicated that its adherence to the Code is communicated to its personnel that the latter is aware of the adherence to the Code in order to adequately handle related Customer inquiries. The Monitoring Body confirmed Temenos's public communication of its adherence to the Code.

The assessment involved the subprocessor management process. Temenos indicated that the CSA contains the terms under which the CSP can engage subprocessors. Based on the information provided by Temenos, a third-party risk management process is in place to ensure that the CSP only engages subprocessors that can provide sufficient guarantees of compliance with the GDPR. Appropriate due diligence, including security, privacy and risk assessments are integrated into the process to evaluate any subprocessors the CSP may engage in Customer Personal Data processing activities.

Another area of focus was built around Data Subject Requests (DSRs). Temenos has implemented self-service functionalities, which allow its Customers to independently handle DSRs. In this regard, Temenos makes available documentation in its Support Portal which outlines how Customers can handle DSRs. Moreover, Temenos has also established internal procedures that enable Customers to request support from CSP's dedicated contact points when assistance with handling DSRs is needed.

When it comes to Customer Audit Rights, Temenos indicated that procedures regarding Customer-requested audits are documented and transparently communicated to Customers. Additionally, Temenos indicated that costs related to exercising Customer Audit Rights are non-prohibitive and non-excessive, which was supported through evidence provided to the Monitoring Body.

Temenos confirmed that all employees and contractors are subject to appropriate confidentiality obligations before being engaged in data processing activities, which continue after the end of the employment or termination of the respective agreements. Training is provided to ensure that personnel involved in the processing of Customer Personal Data are aware of their confidentiality obligations. A security awareness program and additional trainings are also provided to ensure personnel involved in the processing of Customer Personal Data have adequate understanding of organisational policies and procedures.

The Monitoring Body has focused on third country transfers. Temenos indicated that it relies on the appropriate data transfer safeguards as provided by Chapter V GDPR. The Monitoring Body received information from the CSP confirming that Temenos relies on adequacy decisions and Standard Contractual Clauses (SCCs), of which the latter applies overarchingly.

In the context of data breaches, Temenos provided information on its incident management and incident response processes, which are designed to identify, handle and respond to data breaches, should any occur. Temenos explained to the Monitoring Body the key aspects of these processes. The reporting of the data breaches to Customers is a contractual obligation, which is operationalised through relevant policies and procedures.

5 Conclusion

The information provided by Temenos was 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[26] 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[27].

Verification-date: January 2026 **Valid until**: January 2027

Verification-ID: 2023LVL02SCOPE5317

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