temenos

Temenos Cloud Privacy and Security Framework July 2022

Contents

This Temenos Cloud Privacy and Security Framework July 2022 updates and replaces “The Temenos Cloud Services Privacy and Security Framework May 2022”. The key changes are:

- Updating drafting to reflect the application of this Temenos Cloud Privacy and Security Framework to Temenos’ existing client contract structure and future client contract structure.

General Provisions

The provisions of this "**Temenos Cloud Privacy and Security Framework**" (the "**Privacy and Security Framework**") apply to Cloud Services provided by Temenos under either: (i) the General Services Terms and Conditions where your Order Form is governed by the General Service Terms and Conditions or; (ii) the Enterprise Terms and Conditions and the Cloud Services Schedule where your Order Form is governed by the Enterprise Terms and Conditions, (in each case, the "**General Terms**") which utilize the hosting services provided by the hosting provider as specified in the Order Form. This document is subject to change at the discretion of Temenos, however any such change shall (i) only be made in accordance with the Agreement; and (ii) will not result in a material reduction in the protection provided in respect of the Personal Data within the Client Data.

This Privacy and Security Framework may also be referred to as the Temenos Cloud Services Privacy and Security Policy or the security controls / security schedule in the Agreement. Any defined terms used in this Privacy and Security Framework shall have the meanings given to them in the Agreement unless the context requires otherwise.

Temenos and its Affiliates depend on a range of computing and network facilities to process, store and transmit information as part of the provision of Cloud Services to the Client. In view of the opportunities and risks associated with these assets and their importance in protecting the Personal Data, Temenos regards security as a continuous process that forms part of our overall corporate governance and involves all staff members.

This Privacy and Security Framework sets out the security framework under which Temenos will provide the Cloud Services and the approach that will be taken to continuously assess and evolve our specific plans and measures to maintain our controls in response to a rapidly evolving threat environment. For the duration of the Agreement Temenos shall maintain the security procedures and any applicable security related operational controls set out in this Privacy and Security Framework.

Data Protection

This Privacy and Security Framework may operate together with a Data Processing Agreement Schedule (if applicable). In such cases, the Privacy and Security Framework forms the Security Schedule referenced in the Data Processing Agreement Schedule and should be read in conjunction with the Data Processing Agreement Schedule.

Precedence

In case of any conflicting provision in this Privacy and Security Framework and the relevant Agreement, the provision of this Privacy and Security Framework shall prevail if and insofar as the provision relates to the Processing of Personal Data within Client Data by Temenos under the relevant Agreement, unless the Agreement is stricter in terms of such Personal Data Processing, in which case the stricter provision of the Agreement shall prevail.

Existing Contractual Arrangements

For clients and customers who do not have the Agreement as described above (for example: Kony, Avoka and Logical Glue customers prior to 31 March 2020); section 3 of this Privacy and Security Framework sets out the security controls applicable to production cloud based services provided by Temenos and its affiliated companies utilising public cloud hosting providers (such services are referred to under this Privacy and Security Framework as "**Cloud Services**"). Such clients and customers may also have agreed separate data processing arrangements and/or privacy terms with Temenos and its affiliated companies when they entered into their contractual arrangements, in which case such data processing arrangement and/or privacy terms shall prevail.

1. Client Data

1.1 Temenos Responsibilities Regarding Client Data

For products and services within the Infinity family such as from Kony (Quantum / DBX) / Avoka (Journey Manager) / Logical Glue (XAI), additional details are set out in Annex 2.

Temenos will not use the Client Data or derive information from it for any advertising or similar marketing purposes.

Client Data shall not include business contact information, billing details and related information collected from the use of websites of Temenos and/or its Affiliates or the interactions of the Client with Temenos and its Affiliates during the contracting process or to maintain the business relationship with the Client and/or its Affiliates. Temenos' handling of this information is subject to the terms of the Privacy Policy at www.temenos.com.

1.2 Data Controller/Data Processor

The Client shall at all times remain the Data Controller with regard to the Personal Data in the Client Data for the purposes of the Cloud Services.

The Client appoints Temenos as its Data Processor of Personal Data in the Client Data under the Agreement for the purposes of Temenos' provision of the Cloud Services and Temenos shall Process Personal Data in the Client Data in accordance with the Data Processing Agreement Schedule.

1.3 Transfer to Other Countries

In order to provide the Cloud Services in accordance with the Order Form and the Agreement, the Client acknowledges and agrees that Temenos may subject to the terms of the Data Processing Agreement Schedule transfer the Client Data outside the country in which the Client is located unless the Parties have agreed additional terms relating to Client Data that provide otherwise.

The Client Data will be stored "at rest" in the country where the data centre(s) are located as specified in the Order Form.

If Client Data Processed by Temenos to provide the Cloud Services is transferred outside the UK or EU, steps have been taken by Temenos to ensure that all such transfers comply with applicable EU and UK data protection laws. Further information regarding transfers of Client Data from the EU and the UK is available on request.

1.4 Affiliates and Third Party Subcontractors

Some or all of Temenos' obligations under the Agreement may be performed by Temenos Affiliates and the Client agrees as a general authorisation that Temenos may appoint Temenos Affiliates as sub-processors to process Client Data for such purposes provided that Temenos complies with this Privacy and Security Framework. In particular, the Client specifically agrees that the Temenos Affiliates listed in Annex 1 and/or on the Client Portal (as such list is amended from time to time) will act as sub-processors in order to carry out specific Processing activities on behalf of the Client.

The Client also agrees as a general authorisation that Temenos may engage third party subcontractors, which, as part of the subcontractor's role in delivering the Cloud Services, will Process Client Data provided that Temenos complies with the Data Processing Agreement Schedule.

1.5 Client Responsibilities Regarding Client Data

The contractual terms governing the Client's responsibilities with respect to Client Data are set out in the General Terms, the Data Processing Agreement Schedule (for Personal Data), and other applicable terms of the Agreement.

The Client is responsible for determining that the measures set out in this Privacy and Security Framework are appropriate to ensure a level of security appropriate to the risk associated with the processing and the type of data to be protected. The Client may review the privacy and security terms and conditions and limitations, applicable to the service provided by the Hosting Provider, and accepts them as sufficient for the protection of the Client Data transferred to the Hosting Provider.

Some security-related aspects of the Cloud Services are under the control of the Client and in particular, Temenos shall not be in breach of the Agreement to the extent that the liability or breach or Security Incident arises from any Client Controls, including:

a) the Client submits or stores Client Data on systems other than the Temenos Environments that Temenos designates for the storage of Client Data;
b) any person gains access to the Client Data or the Cloud Services through the administration rights, personnel or systems of the Client or the Client's Affiliates;
c) the Client configures the Cloud Services so that Client Data is retained on systems controlled by Temenos for a period longer than is reasonably required by the Client to Process the Client Data as is intended for the specific type of Cloud Services purchased (as further set out in the Documentation). For services where Temenos provides data purging tools, where Client Data is stored for longer than is necessary to meet a legitimate business purpose or for a valid legal purpose;
d) the Client fails to comply with the governance, rules or guidelines relating to the development and distribution of applications via app stores;
e) the Client integrates or requests the integration of the Services with any solutions, services or applications that are not provided by Temenos;
f) the Client uses content, applications or software with the Services other than content, applications or software provided or approved in writing by Temenos or does so in a way which breaches any conditions which Temenos has placed on its approval;
g) the Client fails to adhere to the Temenos upgrade policy for the applicable Temenos Software or fails to implement updates or patches to the Cloud Services in a timely manner that are recommended by Temenos;
h) the Client creates or modifies any Application in a manner that causes Personal Data to appear in the platform services logs;
i) the Client fails to take all reasonable steps to secure Client Data in its possession or control;
j) the Client fails to anonymize or remove Personal Data from Client Data submitted to the Cloud Services or when accessing Support Services notwithstanding contractual obligations or formal requests from Temenos to do so; or
k) the misconfiguration or mismanagement of Applications by the Client or Users.

1.6 Compelled Disclosure of Client Data

In the course of providing its services, Temenos could from time to time receive a law enforcement or government agency request seeking the disclosure of Client Data hosted on Temenos' services. Temenos acknowledges that pursuant to the US Foreign Intelligence Surveillance Act (FISA), Temenos USA entities may be deemed to qualify as an "electronic communication service" and therefore could be subject to the provisions of FISA 702. However, Temenos is not a company that offers telecommunications and/or electronic communications services to the public which are the focus of FISA orders.

Temenos will not disclose Client Data to law enforcement or government agencies and organisations unless compelled by law under a valid binding order (such as a subpoena or court order). Should such agencies and organisations contact Temenos with a demand for Client Data, Temenos will attempt to redirect the agency or organisation to request that data directly from the Client. If compelled to disclose Client Data to the agency or organisation as a matter of law, then Temenos will promptly notify the Client and provide a copy of the demand to enable the Client to seek a protective order or other appropriate remedy to prevent the disclosure unless legally prohibited from doing so.

Temenos will not provide any law enforcement or government agencies with direct or unrestricted access to Client Data, and Temenos offers the Client strong encryption as a standard security feature to ensure that Client Data is protected. This includes encrypting data in transit using appropriate transport layer security (TLS) measures. Further details of the security measures Temenos uses are set out below.

1.7 Client Data Deletion or Return

The General Terms regulate how Client Data shall be handled after expiration or termination of the Client's use of a Cloud Service.

In summary, Temenos will make Client Data available to the Client no later than sixty (60) days after the effective expiration or termination of the Client's use of a Cloud Service. The Client Data will be made available in a secure manner and in text format along with attachments in their native format.

1.8 Data Breach Notification / Security Incident Notification

The General Terms and the Data Processing Agreement Schedule regulate how Security Incidents and Personal Data Security Incidents shall be handled.

The Client must notify Temenos promptly about any possible misuse of its accounts or authentication credentials or any security incident related to any part of the Cloud Services.

Temenos reserves the right to remove access to any channel or interface to the Cloud Services that it reasonably believes to be the source of a Security Incident. Such removal of access shall be notified to the Client and will be classed as an authorised outage in relation to the calculation of any availability of the service to which that channel or interface provides access.

1.9 Non Production Environments, Support Systems and Data

Temenos may offer training, non-production development or test environments or other cloud environments which are not suitable for the management of Client Data ("**Non Production Environments**") for evaluation, development purposes, implementation and internal use. In addition Temenos uses certain systems and portals to provide support for the Software and the Cloud Services and manage support tickets, Change Requests and Service Requests including the Temenos Customer Support Portal ("**Support Systems**"). Non Production Environments and Support Systems may employ lesser or different privacy and security measures than those typically present in the Cloud Services for Production Environments.

Unless otherwise provided, Non Production Environments and Support Systems are not included in the SLA for the corresponding Cloud Service.

Non Production Environments and Support Systems are not designed to be used for the Processing of Personal Data in the Client Data and the Client shall ensure it employs adequate measures to ensure that Personal Data and/or Client Data is not submitted to Non Production Environments and Support Systems. Temenos will inform the Client of environments and Support Systems which are not suitable for Processing of Client Data.

If Client Data is to be submitted in an anonymized format in Non Production Environments or Support Systems, the Client shall approve and validate the tool used for such anonymization and the output of the tool prior to the submission of the anonymized data.

1.10 Support and Support Data

For certain support services, the Client may use the Support Systems including Cloud Service Help Desk, Journey Manager Customer Support Portal, Service Cloud, and Basecamp.temenos.com, which do not use Microsoft Azure or Amazon Web Services. The technical and operational measures set out in section 2 (Security General Technical and Operational Measures) apply to all these support services.

Please note: certain Support Systems such as basecamp.temenos.com are developer portals and public forums and are provided under their own terms of use.

The Client is responsible for ensuring that no Client Data is submitted by its personnel to any ticketing or support systems or to any environments other than to Temenos Production Environments.

The Client shall employ measures to prevent Personal Data being submitted to the support services and/or utilize tools to anonymise (e.g. scramble / mask) the Personal Data.

In certain circumstances, Temenos is also authorised to obtain Client Data from the relevant environments to provide technical support for the Client. In such circumstances, Temenos shall ensure it limits the Personal Data submitted to the support services to the amount necessary to undertake the support and utilizes tools where possible to scramble the Personal Data.

Any Personal Data sent by the Client or Temenos to each other for support purposes shall be transferred using the secure protocol such as FTPS or as agreed between the Parties. The Client confirms that it has the necessary rights to transfer or make available such Personal Data to Temenos under the appropriate legal basis (including that it has or has obtained the consent of the Client's personnel and end users if applicable, or can otherwise justify the disclosure of such Personal Data to Temenos under the relevant Data Protection Laws).

Temenos is not responsible for any Client Data sent using any other storage media except for FTPS and such other secure protocol agreed between the Parties and Temenos shall have no liability for any lost, damaged or destroyed storage media used by the Client.

"**Support Data**" means data, documents and other information relating to the provision of support services forming part of the Cloud Services and may include log files, event files and other trace and diagnostic files that relate to the use and operation of the Cloud Services.

The Client acknowledges that Temenos may use the Support Data and any other information related to the performance, operation and use of the Cloud Services for the following purposes: (i) to ensure the Cloud Services are secure including security monitoring and identity monitoring which may use industry standard tooling; (ii) to administer backup and disaster recovery plans and policies; (iii) to confirm compliance with licensing and other terms of use; (iv) to analyse statistics and other information related to the performance, operation and use of the Cloud Services; and (v) to analyse, develop, improve and optimize services provided by Temenos and its Affiliates provided any such use is in aggregated and anonymized form and shall not contain any Confidential Information of the Client.

Temenos may be responsible for Processing Personal Data provided by or on behalf of the Client that may be incidentally contained in Support Data including Personal Data relating to the representatives, contractors and suppliers of the Client and its Affiliates.

1.11 Location of Client Data at Rest

If applicable, Temenos will store Client Data at rest with its designated Hosting Provider, details of which are set out in the Agreement. Temenos may change the Hosting Provider but only in accordance with the Agreement. Any change of Hosting Provider is not intended to lead to a diminution in service to the Client.

Unless otherwise agreed with the Client elsewhere within the Agreement, Temenos will store Client Data at rest within certain major geographic areas (each, a "**Geo**") as follows:

- If the Client requires a particular service to be deployed within a specific Geo then, where such capability exists and for that service only, Temenos will configure a particular service to store Client Data at rest within the specified Geo. Certain services may not enable the Client to configure deployment in a particular Geo or outside the United States and may store backups in other locations. Further details are available from Temenos upon request, or as may be further specified by the Hosting Provider.

- Unless otherwise stipulated elsewhere in the Agreement, Temenos does not control or limit the regions from which the Client or the Client's end users may access or move Client Data. Any Client requests to alter the specific Geo(s) where Client Data is stored at rest (as stipulated in the Agreement) must be submitted as a Change Request and may incur additional Fees, both in respect of the transfer of Client Data and in respect of the ongoing cost of the Cloud Services (in line with the underlying costs associated with the relevant Geo(s)).

2. Security General Technical and Operational Measures

Described below are the technical and organisational measures undertaken by Temenos in connection with the Processing of Personal Data and performance of its obligations under the Agreement. The technical and organisational measures described in this section 2 and in section 3 are intended to protect the Personal Data against unauthorised Processing and accidental or unauthorised loss, destruction, alteration, disclosure of, or damage to, or access to Personal Data and ensure the protection of the rights of the individual subject to the applicable law.

Prevent unauthorised persons from gaining access to data processing systems on which Personal Data are Processed:

Temenos has implemented physical access control with appropriate measures. The premises are locked using customary measures. Temenos' systems are enclosed by appropriate physical access control measures. For systems that are housed, hosted and maintained by external service providers, Temenos has arranged corresponding measures to be implemented and maintained by these service providers, including access control with login, guidelines for monitoring and identification of guests in the building.

Prevent data processing systems from being accessed, copied, changed or deleted by unauthorised persons:

Temenos has implemented electronic access control using appropriate measures. In particular, access to data processing systems is password protected and multi-factor authentication protected where appropriate and access only granted to authorised persons that are bound to maintain confidentiality and comply with data protection requirements. Temenos has implemented appropriate encryption methods and uses appropriate anti-malware and anti-virus controls to help avoid malicious software gaining unauthorised access to Personal Data. Temenos uses an intelligently structured assignment of permissions and requires that permissions for data access are only assigned to persons who have a need and who are authorised to access them. Temenos requires that persons authorised to use a data processing system only have access to the data covered by their access authorisation and that Personal Data cannot, during Processing or use or after storage, be accessed, read, copied, altered or removed by unauthorised persons.

In the course of electronic transmission or during their transport or storage on a data carrier, Personal Data cannot be read, copied, altered or removed by unauthorised persons, and it is possible to verify and establish to which bodies Personal Data are to be transmitted to by data transmission equipment:

Temenos has implemented transfer control by using appropriate measures, in particular by using an encrypted connection for data access and data transfer over public networks and private networks. Data transfer via internet is only intended where it is absolutely necessary to complete the tasks of Temenos. Client Data is never stored on portable media. Data is only stored on portable media if it is absolutely necessary to complete the tasks of Temenos and, if so, appropriate encryption is applied. Data is not transferred to unknown third parties. Temenos has implemented appropriate measures to ensure the removal of Personal Data from Temenos' systems upon termination of the relevant Agreement, subject to any requirements of applicable law.

It is possible to verify and establish whether and by whom Personal Data have been entered into data processing systems, altered or removed:

Temenos has implemented input control by using appropriate measures. In particular, the systems document who can enter or change data and when. The previous version can always be reestablished if necessary. Data changes are logged. Temenos maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, to whom the breach was reported, and the procedure for recovering data.

Personal Data Processed by sub-processors can only be Processed in conformance with the instructions of the Controlling Party:
Temenos has implemented sub-processor control using appropriate measures, including by entering into written contracts with subcontractors that comply with applicable data protection requirements and including the right to audit the sub-processors' compliance with these agreements.

Personal Data is protected against accidental destruction or loss:

Temenos has implemented processes designed to ensure availability control by using appropriate measures. In particular, Temenos has established and implemented a backup and recovery plan. Backups are created regularly (at least once per day) and Temenos is able to restore data from such backups. Temenos applies appropriate procedures when deleting data to ensure that Personal Data is safely deleted and that Personal Data on media that are no longer in use cannot be retrieved or restored. Temenos requires that all security relevant functions of the processing systems are monitored and available and implements appropriate measures to detect any relevant malfunction without undue delay.

Data which have been collected for different purposes can be Processed separately:

Temenos has implemented the separation rule by using appropriate measures. In particular, such data sets can be identified and separated by the selection functions of the employed system.

The effectiveness of technical and organisational measures for ensuring the security of the Processing of Personal Data is regularly tested, assessed and evaluated:

Temenos regularly tests, assesses and evaluates the effectiveness of the technical and organisational measures, documents the results of such tests, assessments and evaluations and appropriately remedies any deficiency discovered during such tests, assessments and evaluations without undue delay.

Adequate organisational measures to protect Personal Data

Temenos has implemented adequate organisational measures to protect Personal Data. Temenos diligently and adequately chooses, instructs and supervises employees and any other persons involved in the Processing of Personal Data. Temenos has put in place adequate data protection and privacy policies and Temenos verifies and enforces compliance with these policies and the instructions given by Temenos. Employees and other persons involved in the Processing of Personal Data are regularly trained in data protection and privacy. Organisational measures are adequately documented by Temenos.

3. Production Technical and Organisational Measures

Described below are the specific technical and organisational measures that Temenos has implemented when providing the Cloud Services which are used for the Processing of Personal Data in Production Environments. These are applicable to any cloud based services utilising the public cloud provided by Temenos and its Affiliates unless otherwise stated.

Domain	Framework
Application and Interface Security	Client access to the services is defined in the cloud services agreement and forms part of the delivery / implementation of the service. Temenos will provide the Client's third parties access to approved Cloud Services interfaces upon the Client's express authorisation.

	Client access to any interface which is not classified as public is delivered subject to additional access controls, as agreed with the Client in the Order Form or otherwise in writing. Interfaces which are classified as public are protected by Web Application Firewalls and Denial of Service protection. All access to web application and API endpoints is over HTTPS, using modern TLS ciphers. Interfaces used to integrate with third party services are provided in a secure manner using network controls, encrypted protocols and modern authentication mechanisms, such as mTLS, SSH/SFTP, FTPS, IP whitelisting, VPN and similar. All data transmitted through a VPN channel is encrypted, utilizing IPSec network layer encryption or equivalent. Administrative interfaces used for Temenos' management of the service are protected by appropriate controls such as encrypted protocols, VPN, multi-factor authentication, source IP restriction, Temenos managed identities, and Privileged Access Management systems as appropriate. Temenos applications, products or enhancement are subject to Temenos Product Assurance team security testing and approval. Temenos undertakes security testing and scanning procedures for the Temenos Software and interfaces that are aligned with industry standards and best practices such as OWASP or SANS. A combination of manual, dynamic application security testing, and penetration testing is used to identify security vulnerabilities, with high focus on external facing interfaces and APIs. Secure Code Review is performed at product build or verification stage of the SDLC for the purpose of detecting vulnerable or malicious codes. Penetration testing by Temenos is conducted to identify vulnerabilities that might be missed by automated tools. These tests include configuration and deployment, authentication, authorization, session management, input and output validation, error handling, cryptography, business logic testing, and client-side testing.
Audit Assurance and Compliance	Temenos has elected to comply and be certified against a range of industry standards in relation to the delivery of the Cloud Services. Temenos standard external evaluation process includes an annual SOC1, SOC2 and SOC3 attestation examination along with a CSA-CCM compliance assessment, an ISO27001, ISO27017, ISO27018 and ISO22301 certification. The certification and external attestation program is subject to periodic review with scope revalidation to align with internal business and external stakeholder expectations. Temenos will work with the Client should they, or a third party appointed by them, require to undertake an external security test of the Cloud Services. The scope and scheduling of any such testing must be agreed in writing between the Client and Temenos in advance of any such activities being undertaken. Temenos has a dedicated internal audit team that through its audit activity provides reasonable assurance that the Cloud Services and operational controls meet the defined standards as outlined in Temenos policies and procedures.

Business Continuity Management and Operational Resilience	Temenos maintains plans for the continuity of business services and where appropriate (i.e. UAT / Live) technical platforms are provided in relation to the Cloud Services. Continuity measures include the use of multiple data centre locations, data backup and synchronization, use of high availability measures, ability to perform operational and support activities from multiple locations. These plans along with business impact analysis are revisited and updated annually. The BCP team conducts testing of the business continuity and disaster recovery plans for critical services, per the defined testing schedule for different loss scenarios. Issues identified during testing are resolved and plans are updated accordingly. Additional tests are performed to cover testing of internal tools used in the delivery of services. As a mandatory requirement, cloud production instances for critical core banking services are tested once every 12 months (this is not applicable to Journey Manager or XAI). Data Backups are secured with a full disk encryption mechanism and secure key handling, Temenos has implemented transparent data encryption (TDE) in Azure databases. Archived Backups are not undertaken for any other environment except for Live. Backups of systems are retained, as per contractually agreed retention period, to be used for restoration in the event of a disaster. Backups of applications are performed on a regular basis where applicable. Backup restoration tests are performed on a regular basis to ensure recovery capability. Uninterruptible Power Supply ('UPS') and diesel generators are installed in the facilities where appropriate. Preventive maintenance is performed on a regular basis.
Change Control and Configuration Management	Temenos operates a Change and Release Management Policy that includes Classification of Changes based on impact, complexity and risk, Testing, Evaluating and Authorizing of Changes, Scheduling of Changes, and Communication of Changes to internal and external parties, and Monitoring of Changes. Change requests are raised by the support teams, assessed for Impact, reviewed and approved by Change Advisory Board prior to release. A repository of applied changes along with post implementation analysis and result is maintained for Cloud Services support team records. Changes impacting infrastructure, networks, access control, and security controls are subject to approval by the Temenos Security Team. Temenos develops an appropriate promotional model for each service. This promotional model caters for verification activities undertaken by Temenos (regression testing, security testing, performance testing) as well as those undertaken by the Client (systems integration testing, UAT, training) where applicable (this is not applicable to XAI). Temenos maintains a repository of all configuration item data as well as any changes to that configuration. Version control and automation are used to standardize the deployment of environments and any changes to those environments.

Data Security and Information Lifecycle Management	Temenos has implemented an Information Classification Policy which identifies and classifies information based on confidentiality, availability and Integrity. Protection requirements, access restrictions, retention, and destruction principles are defined and applied as mandated. Temenos classifies any asset which contains Client Data to help identify it, and ensure that access is appropriately restricted, that any data retained is approved by the Client (except where Temenos is required by law to retain the data), and the use of the data is required for the purposes of providing Cloud Services. Temenos has specific process for Client Data handling, such as to ensure production data is not used in its system design and testing environments, Client Data transfer is restricted to approved channels. Client Data is encrypted at rest and in transit at all times. Temenos has documented procedures in relation to the destruction and sanitization of any asset or media which contains Client Data, including both electronic and physical copies of that data. All transferred, disposed or recycled assets (electronic devices, media, computer systems etc.) are sanitized of confidential / sensitive data and software (following NIST guidelines) or destroyed.
Datacentre Security	Temenos limits access to Temenos controlled facilities, where information systems that process Client Data are located, to identified and authorised individuals. Physical access to Temenos controlled facilities is monitored for restricting unauthorized access and recorded. Closed Circuit Television (CCTV) cameras are placed to monitor personnel entry and exit points. Data centre facilities are provided by the Hosting Provider (for example Microsoft Azure) which will have in place its security measures in line with industry standards. Further details of the data centre facilities provided by the Hosting Provider are available from Temenos upon the Client's written request.
Encryption Key Management	Client Data is encrypted at rest using modern encryption algorithms and secure key management processes. Encryption may be at the block, database, table, or row level depending on service and requirements. Access to encryption cryptographic keys is restricted on a 'need to know' basis to the fewest number of custodians as necessary. All staff are subject to confidentiality arrangements. Staff having access to keys must sign to an approved confidentiality arrangement. Only authorised systems, applications, processes or users should have access to encryption cryptographic keys. Development environments do not have access to, nor knowledge of, Production Environment cryptographic key materials. Developers must not be assigned responsibilities of production key custodians. Cryptographic keys are never transmitted or stored in the clear. Cryptographic keys are protected against loss of confidentiality, integrity and availability. Temenos has developed Key Compromise procedures that specify steps to be taken in the event of encryption key compromise, including revocation, rotation, and communication to affected parties.

Governance and Risk Management	Temenos Cloud Services Risk Management Board Committee has responsibility among others to: 1. review and approve risk management strategy, policy and framework ensuring alignment with Temenos Group policy; 2. review results and quality of risk assessments performed; 3. ensure that all material risks have defined owners, treatment plans and implementation progress is monitored; and 4. review and approve initiatives to implement risk management practices within existing operations and provide insight, guidance and sponsorship for delivery of such initiatives. The Temenos Cloud Services Risk Management Board Committee meets quarterly at the minimum or as often as it may be required. A formal risk assessment exercise is carried out on a regular basis to identify new or changed risks causing disruption to cloud services and suitable mitigation plans are developed to address those risks. The status of risk treatment plans is monitored until risks are mitigated to an acceptable level. In response to the identification of such risks, management updates, as needed, its policies, procedures, processes and controls.
Human Resources	Temenos has procedures and security measures in place to manage employment lifecycle from on-boarding through termination, including for any changes in employees' role or responsibilities. Measures may include but not limited to adequate screening, contracting, training, evaluation, clearance and off boarding. Temenos conducts screening of employee suitability in accordance with a "Background Check" policy and process that specifically extends to an employee, selected candidate, or third parties whose roles require physical or logical access to production environments containing Client Data. Screening is conducted prior to on-boarding and where appropriate regularly during employment lifecycle. Temenos is committed to ethical and lawful business conduct. Corporate policies and trainings, that include Information Systems Security Policy and awareness training, Data Protection and Privacy, Business Code of Conduct, Anti-Corruption and Bribery, are taken and acknowledged during on-boarding and annually thereafter. In addition, an annual refresher training is conducted for Cloud personnel to enforce awareness of security and privacy measures and personnel responsibilities in relation to services provided in cloud.
Identity and Access Management	Temenos operates an Identity and Access Management policy which defines the logical and physical access requirements to Cloud Services environments. Access is provided on a 'least privilege' basis, with all access requiring a 'business justification' while maintaining 'segregation of duties'. All changes to access are controlled via a standard process. Records of requests for individuals having access to Client Data, including security privileges, approvals and changes are maintained. Temenos ensures that segregation of duties exists between access requester, approver, and implementer. Temenos uses industry standard practices to identify and authenticate users who attempt to access information systems, such as passwords and multi-factor authentication. Password based access must adhere to the Temenos Password Policy, which defines the complexity, rotation timeframe, history, and lockout duration criteria for passwords and is enforced on all workstations in the Temenos processing area by the IT team. Temenos audits entitlement to access rights and roles on a quarterly basis to ensure that processes and procedures in relation to Joiners, Movers, and Leavers is followed,

	that exceptions are reported and corrected, and to validate that entitlements are still appropriate for the role or function being delivered. Management of Temenos Cloud Services is conducted from Temenos cloud clean rooms. The physical access to these rooms is restricted to authorised Temenos personnel only.
Infrastructure and Virtualisation Security	Temenos follows a strategy of defence-in-depth in the design and implementation of the infrastructure used to provide the Cloud Services. Temenos has defined and maintains applicable hardening standards for systems and infrastructure components based on CIS Benchmarks and industry best practice. These standards include: • Removal of system functionality that is not required • Changing of default passwords, disabling of guest accounts • Default-deny network security rules, only permitting traffic necessary to deliver the services Temenos segregates Production Environments and Non-Production Environments and has controls in place to ensure that Client Data is not transferred to an environment that the Client has not authorised it for. Access to the administrative area for the control of the virtual environments is restricted and segregated from access to the specific Client environments. Documentation detailing networks and servers are maintained for each environment.
Security Incident Management, E-Discovery, and Cloud Forensics	Temenos has implemented a Security Incident Management process for early detection and adequate management of potential security incidents including their containment and third-party communication protocols. A record of security incidents is adequately maintained. Temenos has formed the Security and Privacy Committee whose primary role is to oversee management effort in implementing global information security and privacy compliance programs within the Temenos Group. Committee responsibility includes an assessment of all security incidents, including incidents that may result in the breach of Personal Data, contain them and take immediate action in order to rectify the situation. Temenos Information Security team works alongside the Security and Privacy Committee and the Product Security team in order to develop and oversee the implementation of information security controls. Temenos IT Security and Awareness training is part of mandatory trainings to be taken by Temenos employees and contractors during their first weeks of joining and annually thereafter. In addition, an enhanced annual refresher training is conducted specifically for Cloud Services Team personnel covering the aspects of security and privacy around cloud services.
Supply Chain Management, Transparency and Accountability	Temenos enters into agreements with third party vendors that include defined scope of services, contractual terms and conditions, SLAs, provider responsibilities including compliance with Temenos Data Protection, Privacy and IT Security, Anti bribery and Corruption, Confidentially or Non-Disclosure requirements. As part of the Temenos Group commitment to enhance the compliance programs, Temenos defined the Supplier Code of Conduct that is communicated and undertaken to adhere to by Temenos vendors.

	Temenos conducts vendor due diligence and risk assessment exercises prior to on-boarding and annually thereafter. An internal scoring system and assessment matrix is used to evaluate risk exposure. Where needed risk-mitigating recommendations are provided by Temenos for inclusion in the vendor agreement.
Threat and Vulnerability Management	Temenos adopts a layered approach (defence-in-depth) using multiple sets of controls to protect against and react to threats and vulnerabilities. Threats and vulnerabilities are detected and remediated via a number of controls that are present in all Temenos Environments containing Client Data. These are: • Patch Management programme to ensure timely delivery of security patches for operating systems and services. • Vulnerability assessment and remediation to address vulnerabilities in components, configuration, and services. • Periodic penetration testing of Production Environments via non-destructive means, taking due care not to impact delivery of the services in accordance with the Temenos Cloud Penetration Testing procedure. Threat protection to detect and block suspicious access to cloud resources used to deliver the service, akin to intrusion detection and prevention. • Anti-virus / anti-malware technology on Microsoft Windows based systems. Data Loss Prevention controls are present on all Temenos employee computing devices used to implement, access, and manage cloud environments containing Client Data. These controls monitor, alert, and block the movement or transfer of sensitive information. Temenos operates a Cyber Threat Intelligence programme to identify and monitor external security threats which have the potential to impact Temenos systems and services, and coordinates with system and service owners to ensure necessary actions as taken.
Client Configuration	Data Retention Certain Temenos Cloud Services come with the ability for Clients to configure data retention to their own requirements. Details of these configurations are available in the Documentation. Integration Some Temenos Cloud Services can be integrated with third party service offerings that complement and extend the service. Integration with third party services is done in a secure manner using network controls, encrypted protocols and modern authentication mechanisms, such as mTLS, IP whitelisting, and similar. More details are available in the Documentation and integration may be subject to additional fees or specific terms in the Order Form.

4. Certifications and Audits

The methodologies and processes adopted by Temenos in the provision of the Cloud Services adhere to widely recognized international standards and principles that are regularly audited and certified by reputable accredited bodies.

Temenos as a cloud services business provider has elected to undergo periodic external examinations in order to ensure its processes and controls maintains compliance with various standards and practices that are applicable to service providers managing customer data in the cloud.

As of July 2022 Temenos maintains the following certifications and annual attestations:

- **ISO/IEC 27001:2013** standard certification in relation to the establishment, implementation, control, and improvement of the Information Security Management System for its office sites for Product Analysis and Customer Support, hosting business, Temenos Application Management & Shared Service Centre and related support processes. An external surveillance audit extended to all ISO27001 mandated requirements is conducted at least annually to ensure controls and process maintains their effectiveness throughout the 3 year certification period.

  The ISO/IEC 27001:2013 certification for hosting business has been further enhanced with:

  - **ISO/IEC 27017:2015** standard for "Information security controls for cloud services"; and
  - **ISO/IEC 27018:2019** standard for "Protecting of Personally Identifiable Information (PII) in public cloud".

- **ISO/IEC 22301:2019** standard certification for Business Continuity Management system that proves for a successfully implemented, robust and comprehensive process.
- **ISO/IEC 20000-1:2018** standard certification for Information Technology, Service Management system requirements.
- **AICPA/SSAE 18 – SOC 2** attestation of operational controls including compliance with Cloud Security Alliance – Cloud Control Matrix (CSA-CCM) Temenos hosting business undergoes annual attestation to ensure its processes and controls maintains compliance with standard mandated requirements relevant to data security, availability, confidentiality, privacy and processing integrity trust service criteria.
- **AICPA – SOC1** attestation of application development, testing, maintenance, quality assurance, production support and related IT general controls and their suitability to achieve organization control objectives.
- **AICPA – SOC3** attestation designed to meet the needs of general users such as client employed third parties other than auditors or regulators. The SOC3 public report includes the assertion and auditor opinion on whether Temenos cloud services controls relevant to security, availability, processing integrity, confidentiality and privacy were effective throughout the audit period.

For detailed location specific certification and attestation coverage, please refer to Annex 1 of this Privacy and Security Framework. The certifications set out in above in this Section 4 (Certification and Audits) and in Annex 1 of this Privacy and Security Framework do not apply to XAI and Logical Glue.

Certification and external attestation scope is subject to annual review and validation as this requires alignment with business expansion.

Temenos will provide the annual attestation reports (AICPA/SSAE18 SOC1, AICPA/SSAE18 SOC2) and the certificates to the Client so that the Client can reasonably verify Temenos' compliance with its security and privacy obligations. The attestation reports are Temenos and Auditor confidential information and may be subject to additional confidentiality undertakings.

Microsoft as Hosting Provider

For further information regarding how the Hosting Provider manages security and privacy in relation to Client Data held in Azure please see the following links for Microsoft Azure:

- https://www.microsoft.com/en-us/trust-center/product-overview
- https://www.microsoft.com/en-us/trust-center/privacy?rtc=1

For further information about Microsoft's subcontractors, please see the following link:

- https://www.microsoft.com/en-us/trust-center/privacy/data-access?rtc=1#subcontractors

Amazon Web Services as a Hosting Provider

For further information regarding how the Hosting Provider manages security and privacy in relation to Client Data held in Amazon Web Services please see the following links:

- https://aws.amazon.com/security/
- https://aws.amazon.com/privacy/

For further information about Amazon Web Service's subcontractors, please refer to the following link:

- https://aws.amazon.com/compliance/sub-processors/

For other Hosting Providers, please contact Temenos.

How to Contact Temenos

If the Client believes that Temenos is not adhering to its privacy or security commitments, the Client may contact Client support, its Temenos representative or account manager or write to Temenos' mailing address at: **Temenos Headquarters SA / Temenos Cloud Switzerland SA, 2, rue de L'Ecole-de-Chimie, 1205 Geneva, Switzerland, Attn**: **General Counsel**.

Annex 1

List of Temenos Group Affiliates which may be engaged to provide continuity of services as at July 2022

Please note that the Temenos Group may provide updates to this list from time to time.

IMPORTANT NOTE: COVID-19 PANDEMIC*

Owing to the unprecedented nature of the Covid-19 pandemic, the Temenos security controls and service delivery model may have to change at short notice in response to measures put in place by governments and/or authorities. Any such changes shall only apply for as long as is reasonably necessary, and only to the extent necessary.

Whilst Temenos will endeavour to provide as much notice as possible to Clients of any changes to the Temenos service delivery model, the situation around the globe is evolving rapidly such that it may not be possible to give the Client the same degree of notice as Temenos would normally provide. The priority of Temenos throughout this crisis will be the continuity and security of critical services.

In accordance with government advice and restrictions in different countries, there is a growing need to work flexibly and from home so that Temenos can continue to provide services and keep everyone safe.

All employees working remotely from home or otherwise outside of an office location are required to connect securely to our network before undertaking activities involving the management of the services provided to Clients.

For critical services, Temenos will endeavour to operate from the office location which usually provides those critical services (to the extent that local conditions and government restrictions allow). In the event that this office is unavailable (for example due to a suspension of movement or a mandated closure of offices) arrangements are in place for those critical services to either be delivered by trained staff based at another of the office locations listed in Annex 1, or to be delivered by specific senior staff operating from home using secure, Temenos issued equipment.

*This notice is deemed to be sent to the Client or Customer on behalf of the relevant Temenos Group contracting entity, which may include a Kony or Avoka entity. This notice replaces the list in Annex 1 of the Temenos Cloud Services Privacy and Security Framework (formerly the Temenos Cloud Services Privacy and Security Policy) where applicable.

For Clients within the European Economic Area, UK and Switzerland

If the Client is located within the European Economic Area, the UK or Switzerland Temenos may:

(a) subcontract any part of its obligations under the Agreement to the Temenos Affiliates listed in the table below; and

(b) only engage as sub-processors of Personal Data in the Client Data the Temenos Affiliates listed in the table below which are located: (i) within the same location as the Client; (ii) within the European Economic Area, the UK or Switzerland; (iii) within India (except for Kony IT Services Pvt Ltd which shall not be engaged as a sub-processor); (iv) within Australia; or (v) if applicable, within the USA by Kony Inc solely with respect to providing technical support for Temenos Quantum hosted by Amazon Web Services.

TEMENOS AFFILIATES

Location	Company	Address	Site Certification and Attestation
Australia	Temenos Australia Operations Pty Ltd Temenos Australia Services Pty Ltd.	Level 10 85 Castlereagh Street Sydney NSW 2000	ISO/IEC 27001:2013 ISO/IEC 27017:2015 ISO/IEC 27018:2019 ISO/IEC 9001:2015 ISO/IEC 22301:2019 AICPA/SSAE18 - SOC2 Type 2 for Security, Processing Integrity, Confidentiality, Availability and Privacy including CSA-CCM compliance AICPA SOC1 Type 2 AICPA SOC3
Australia	Avoka Technologies Pty Ltd	Level 2 1a Rialto Lane Manly, NSW 2095	ISO/IEC 27001:2013 ISO/IEC 27017:2015 ISO/IEC 27018:2019 AICPA/SSAE18 - SOC2 Type 2 for Security, Processing Integrity, Confidentiality, Availability and Privacy including CSA-CCM compliance AICPA SOC1 Type 2 AICPA SOC3
Belgium	Temenos Belgium SA	Parc du Nysdam Avenue Reine Astrid 92 1310 La Hulpe BELGIUM	-
India	Temenos India Private Ltd	Sterling Road n°146 Nungambakkam Chennai 600 034	ISO/IEC 27001:2013 ISO/IEC 27017:2015 ISO/IEC 27018:2019 ISO/IEC 9001:2015 ISO/IEC 22301:2019 ISO/IEC 20000-1:2018 AICPA/SSAE18 - SOC2 Type 2

		KG 360°- IT Business Park Second Floor N° 232/1 Dr MGR Salai, Perungudi Chennai 600 096 IBC Knowledge Park Block C & D 3rd & 11th Floor No. 4 / 1, Bannergatta Road, Near Dairy circle, Bangalore 560029 India	for Security, Processing Integrity, Confidentiality Availability and Privacy including CSA- CCM compliance AICPA SOC1 Type 2 AICPA SOC3
	Kony India Private Ltd	SEZ – Unit II, Level 7 Building No. H06 Hitech City 2 Phoenix Info City Gachibowli Serilingampally Hyderbad, Hyderbad TG 500081	ISO/IEC 27001:2013 ISO/IEC 27017:2015 ISO/IEC 27018:2019 ISO/IEC 22301:2019 AICPA/SSAE18 - SOC2 Type 2 for Security, Processing Integrity, Confidentiality Availability and Privacy including CSA- CCM compliance AICPA SOC1 Type 2 AICPA SOC3 PCI- DSS (Azure and AWS) environment
	Kony IT Services Pvt Ltd	9th Floor, B 6 – South Tower Divyasree Orion Sy.No.66/1 Raidurgam Hyderabad TG 50031	ISO/IEC 27001:2013 ISO/IEC 27017:2015 ISO/IEC 27018:2019 ISO/IEC 22301:2019 ISO/IEC 20000-1:2018 AICPA/SSAE18 - SOC2 Type 2 for Security, Processing Integrity, Confidentiality Availability and Privacy including CSA- CCM compliance AICPA SOC1 Type 2 AICPA SOC3 PCI- DSS (Azure and AWS) environment
Romania	Temenos Romania SRL	319G, Splaiul Independentei Atrium House Ground Floor 2nd Floor and 3rd Floor 6th District Bucharest 060044 Romania	ISO/IEC 27001:2013 ISO/IEC 27017:2015 ISO/IEC 27018:2019 ISO/IEC 9001:2015 ISO/IEC 22301:2019 AICPA/SSAE18 - SOC2 Type 2 for Security, Processing Integrity, Confidentiality, Availability and Privacy including CSA-CCM compliance AICPA SOC1 Type 2 AICPA SOC3

Switzerland	Temenos Headquarters SA Temenos Cloud Switzerland SA	2 rue de l'Ecole-de-Chimie, 1205 Geneva	-
United Kingdom	Temenos UK Ltd	71 Fenchurch Street (5th Floor) London EC3M 4TD	ISO/IEC 27001:2013 ISO/IEC 27017:2015 ISO/IEC 27018:2019 ISO/IEC 9001:2015 ISO/IEC 22301:2019 AICPA/SSAE18 - SOC2 Type 2 for Security, Processing Integrity, Confidentiality, Availability and Privacy including CSA-CCM compliance AICPA SOC1 Type 2 AICPA SOC3
United States	Kony Inc.*	9225 Bee Caves Rd. Building A, Suite 300 Austin, Texas 78733	ISO/IEC 27001:2013 ISO/IEC 27017:2015 ISO/IEC 27018:2019 AICPA/SSAE 18 - SOC2 Type 2 for Security, Processing Integrity, Confidentiality, Availability and Privacy including CSA-CCM compliance AICPA SOC1 Type 2 AICPA SO3 PCI- DSS (Azure and AWS infrastructure)

Every Temenos Affiliate listed above is not necessarily undertaking activities for each Client or Customer. The activities undertaken by each entity for a specific Client or Customer are available upon request from Temenos.

*Solely with respect to providing technical support for Temenos Quantum hosted by Amazon Web Services.

For Clients located outside of the European Economic Area, the UK and Switzerland

If the Client is located within a location other than within the EEA, UK or Switzerland Temenos may:

(a) subcontract any part of its obligations under the Agreement to the Temenos Affiliates listed in the table below; and

(b) engage as sub-processors of Personal Data in the Client Data the Temenos Affiliates listed in the table below.

TEMENOS AFFILIATES

Location	Company	Address	Site Certification and Attestation
Australia	Temenos Australia Operations Pty Ltd Temenos Australia Services Pty Ltd.	Level 10 85 Castlereagh Street Sydney NSW 2000	ISO/IEC 27001:2013 ISO/IEC 27017:2015 ISO/IEC 27018:2019 ISO/IEC 9001:2015 ISO/IEC 22301:2019 AICPA/SSAE18 - SOC2 Type 2 for Security, Processing Integrity, Confidentiality, Availability and Privacy including CSA-CCM compliance AICPA SOC1 Type 2 AICPA SOC3
Australia	Avoka Technologies Pty Ltd	Level 2 1a Rialto Lane Manly, NSW 2095	ISO/IEC 27001:2013 ISO/IEC 27017:2015 ISO/IEC 27018:2019 AICPA/SSAE18 - SOC2 Type 2 for Security, Processing Integrity, Confidentiality, Availability and Privacy including CSA-CCM compliance AICPA SOC1 Type 2 AICPA SOC3
Belgium	Temenos Belgium SA	Parc du Nysdam Avenue Reine Astrid 92 1310 La Hulpe BELGIUM	-
Costa Rica	Temenos Costa Rica SA	Sabana Norte Avenida 5 calles 42 y 44 Edificio Nueva #4260 Segundo Pis	ISO/IEC 22301:2019 ISO/IEC 20000-1:2018 AICPA/SSAE18 - SOC2 Type 2 for Security, Processing Integrity, Confidentiality, Availability and Privacy including CSA-CCM compliance AICPA SOC1 Type 2 AICPA SOC3

Ecuador	Temenos Ecuador SA	Orellana 500 Calle Orellana 1349 Benalcázar, Quito Ecuador	ISO/IEC 22301:2019 ISO/IEC 20000-1:2018 AICPA/SSAE18 - SOC2 Type 2 for Security, Processing Integrity, Confidentiality, Availability and Privacy including CSA-CCM compliance AICPA SOC1 Type 2 AICPA SOC3
India	Temenos India Private Ltd	Sterling Road n°146 Nungambakkam Chennai 600 034 KG 360°- IT Business Park Second Floor N° 232/1 Dr MGR Salai, Perungudi Chennai 600 096 IBC Knowledge Park Block C & D 3rd & 11th Floor No. 4 / 1, Bannergatta Road, Near Dairy circle, Bangalore 560029 India	ISO/IEC 27001:2013 ISO/IEC 27017:2015 ISO/IEC 27018:2019 ISO/IEC 9001:2015 ISO/IEC 22301:2019 ISO/IEC 20000-1:2018 AICPA/SSAE18 - SOC2 Type 2 for Security, Processing Integrity, Confidentiality Availability and Privacy including CSA- CCM compliance AICPA SOC1 Type 2 AICPA SOC3
	Kony India Private Ltd	SEZ – Unit II, Level 7 Building No. H06 Hitech City 2 Phoenix Info City Gachibowli Serilingampally Hyderbad, Hyderbad TG 500081	ISO/IEC 27001:2013 ISO/IEC 27017:2015 ISO/IEC 27018:2019 ISO/IEC 22301:2019 AICPA/SSAE18 - SOC2 Type 2 for Security, Processing Integrity, Confidentiality Availability and Privacy including CSA- CCM compliance AICPA SOC1 Type 2 AICPA SOC3 PCI- DSS (Azure and AWS) environment
	Kony IT Services Pvt Ltd	9th Floor, B 6 – South Tower Divyasree Orion Sy.No.66/1 Raidurgam Hyderabad TG 50031	ISO/IEC 27001:2013 ISO/IEC 27017:2015 ISO/IEC 27018:2019 ISO/IEC 22301:2019 ISO/IEC 20000-1:2018 AICPA/SSAE18 - SOC2 Type 2 for Security, Processing Integrity, Confidentiality Availability and Privacy including CSA- CCM compliance AICPA SOC1 Type 2 AICPA SOC3 PCI- DSS (Azure and AWS) environment

	Kony Services India, LLP	Building No 9B, Part of 5th Floor Survey No. 64 (part), Mindspace, Madhapur, Serilingampally (M) Hyderbad Rengareddi TG 500081		-
Luxembourg	Temenos Luxembourg SA	21 rue du Puits Romain L-8070 Bertrange LUXEMBOURG		-
Mexico	Temenos Mexico SA de CV	Paseo de la Reforma 505 Floor 15 - Suite D, Colonia Cuauhtemoc C.P. 06500 Méxic DF	ISO/IEC 22301:2019 ISO/IEC 20000-1:2018 AICPA/SSAE18 - SOC2 Type 2 for Security, Processing Integrity, Confidentiality, Availability and Privacy including CSA-CCM compliance AICPA SOC1 Type 2 AICPA SOC3	
Netherlands	Kony Solutions B.V	Kabelweg 37 1014BA Amsterdam		-
Poland	Temenos Polska sp.zo.o.	Metropolitan Building 4th Floor, Pl.Piłsudskiego 1, 00078 Warszawa		-
Romania	Temenos Romania SRL	319G, Splaiul Independentei Atrium House Ground Floor 2nd Floor and 3rd Floor 6th District Bucharest 060044 Romania	ISO/IEC 27001:2013 ISO/IEC 27017:2015 ISO/IEC 27018:2019 ISO/IEC 9001:2015 ISO/IEC 22301:2019 AICPA/SSAE18 - SOC2 Type 2 for Security, Processing Integrity, Confidentiality, Availability and Privacy including CSA-CCM compliance AICPA SOC1 Type 2 AICPA SOC3	
Singapore	Temenos Singapore Pte Ltd Kony Singapore Pte Ltd	5 Shenton Way #18-01 UIC Building Singapore 068808		-
Switzerland	Temenos Headquarters SA Temenos Cloud Switzerland SA	2 rue de l'Ecole-de-Chimie 1205 Geneva		-

United Kingdom	Temenos UK Ltd	71 Fenchurch Street (5th Floor) London EC3M 4TD	ISO/IEC 27001:2013 ISO/IEC 27017:2015 ISO/IEC 27018:2019 ISO/IEC 9001:2015 ISO/IEC 22301:2019 AICPA/SSAE18 - SOC2 Type 2 for Security, Processing Integrity, Confidentiality, Availability and Privacy including CSA-CCM compliance AICPA SOC1 Type 2 AICPA SOC3
United States	Temenos Cloud Americas LLC	40 General Warren Blvd, Suite 200 Malvern, PA 19355 USA	ISO/IEC 22301:2019 ISO/IEC 20000-1:2018 AICPA/SSAE18 - SOC2 Type 2 for Security, Processing Integrity, Confidentiality, Availability and Privacy including CSA-CCM compliance AICPA SOC1 Type 2 AICPA SOC3
	Temenos USA Inc	40 General Warren Blvd, Suite 200 Malvern, PA 19355 USA	-
	Kony Inc.*	9225 Bee Caves Rd. Building A, Suite 300 Austin, Texas 78733	ISO/IEC 27001:2013 ISO/IEC 27017:2015 ISO/IEC 27018:2019 AICPA/SSAE 18 - SOC2 Type 2 for Security, Processing Integrity, Confidentiality, Availability and Privacy including CSA-CCM compliance AICPA SOC1 Type 2 AICPA SOC3 PCI- DSS (Azure and AWS infrastructure)
	Avoka (Usa), Inc	385 Interlocken Cres Ste 1050 Broomfield, CO, 80021-3492	ISO/IEC 27001:2013 ISO/IEC 27017:2015 ISO/IEC 27018:2019 ISO/IEC 22301:2019 ISO/IEC 20000-1:2018 AICPA/SSAE18 - SOC2 Type 2 for Security, Processing Integrity, Confidentiality, Availability and Privacy including CSACCM compliance AICPA SOC1 Type 2 AICPA SOC3

Every Temenos Affiliate listed above is not necessarily undertaking activities for each Client or Customer. The activities undertaken by each entity for a specific Client or Customer are available upon request from Temenos.

*Solely with respect to providing technical support for Temenos Quantum hosted by Amazon Web Services.

External Sub-processors of Client Data

Microsoft and its subcontractors	Hosting Provider – if identified in applicable Order Form
Amazon Web Services and its subcontractors	Hosting Provider – if identified in applicable Order Form

ANNEX 2

Logical Glue / XAI Additional details:

The Client acknowledges and agrees that it is not necessary for the performance of the Cloud Services to provide any Client Data to Temenos, and in particular no Personal Data is required. The Client shall ensure it shall not disclose, submit or otherwise make any Personal Data available to Temenos unless such data has been irreversibly anonymised beforehand in such a manner that the data subject is not or is no longer identifiable. If the scope of Cloud Services changes during the term of the Agreement and Temenos will need to process Personal Data for and on behalf of the Client as part of such extended Cloud Services, then Temenos shall only process the Personal Data as a data processor on behalf of the Client in accordance with the Client's documented instructions and the parties will agree a data processing addendum before the commencement of such Cloud Services.