Client Considerations Regarding SOC2, GDPR, ISO and PCI Compliance

January 2023

TABLE OF CONTENT

OpenLegacy's Position

OpenLegacy's platform and generated code only act as a pipe to pass data between the client's legacy system and databases and modern frontends (whether private or public) and does not store or persist any client, financial, confidential, personal data. Therefore, SOC 2, GDPR, and PCI regulations do not apply to the OpenLegacy platform, its libraries, or generated microservices.

This position statement demonstrates this claim through reference architecture diagrams and detailed explanations.

OpenLegacy understands and recognizes the importance of "information" to its business operations and hence is committed to provide its customers, stakeholders, business partners & employees a secure information processing environment.

OpenLegacy intends to achieve security of its information assets based on the three founding principles of Information Security - Confidentiality, Integrity & Availability.

Optimum security will be accorded to information assets by classifying them based on their business value and risk exposure.

OpenLegacy thus will ensure the privacy of company, customer, stakeholder, business partner & employee information, by protecting it against unauthorized access, disclosure and/or loss.

OpenLegacy endeavors to continuously and proactively manage risk to its information at an acceptable level through the design, implementation and maintenance of an effective Information Security Management System (ISMS) that adopts industry best practices & standards.

The ISMS so developed will comply with the requirements of the national laws and regulatory requirements.

The need for ISMS will be highlighted by encouraging and promoting information security awareness amongst the masses at The Company.

It is the policy of OpenLegacy to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information.

In addition, it is the policy of OpenLegacy to protect information belonging to third parties that has been entrusted to OpenLegacy in a manner consistent with its sensitivity as well as in accordance with all applicable agreements.

The principles that shall be followed to secure the information are as follows:

- Securing of information based on the three founding principles of Information Security - Confidentiality, Integrity & Availability, to facilitate appropriate sharing of information across the organization.
- Ensuring the privacy of Organization, customer, stakeholder, business partner & employee information by suitable protection of the information and its information processing infrastructure against threats, both internal and external.
- Continuously and proactively monitoring and managing the risks based on the The Company's risk appetite.
- Maintaining an effective Information Security Management System (ISMS) which adopts leading industry standards and best practices to ensure the security of information by providing a framework of learning & innovation and by challenging existing practices and introducing new processes and practices.
- Promoting awareness amongst customers, business partners, stakeholders and employees by sharing knowledge and responsibility.
- Ensuring that all the government laws and regulatory requirements are complied with.

Reviewing and aligning the Information Security Policy with The Company's business objectives and communicate the changes (if any) to all concerned on a regular basis.

The Security Policy will be reviewed independently once in a year or earlier if circumstances require. It will be published and communicated to all employees and relevant external parties and any non-conformity will be addressed to ensure compliance.

The overall responsibility for ensuring that the Policy is implemented, developed and reviewed effectively rests with the Chief Executive Officer.

This responsibility will be delegated throughout the management structure reflecting our continued commitment to Security at all levels throughout The Company.

This statement represents our general position on Information Security issues, and the policies and practices we will apply in conducting our business.

Compliance Definitions

1.1 SOC 2

SOC 2 is an auditing procedure designed to ensure that service providers storing customer data in the cloud, manage that data securely. In effect this means SOC 2 applies to nearly every SaaS company, as well as any company that stores its customers' information on the cloud.

1.2 GDPR

The General Data Protection Regulation (GDPR) is part of the EU laws that govern data protection and privacy for citizens of the (EU). It also addresses the transfer of personal data outside the EU. GDPR provides a well-defined mechanism for individuals to control their personal data and simplifies the regulatory environment by unifying the regulation within the EU.

1.3 PCI DSS

Payment Card Industry Data Security Standard (PCI DSS) is a set of global policies and procedures developed to protect payment systems handling credit, debit and cash card transactions. It prevents the misuse of cardholders' personal information and security breaches and data theft from the payment systems. PCI DSS compliance is required of all vendors by all credit, debit and cash card brands.

1.4 ISO 27001

ISO 27001 is a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes.

OpenLegacy Compliance

1.5 Reference Architecture Example - CICS

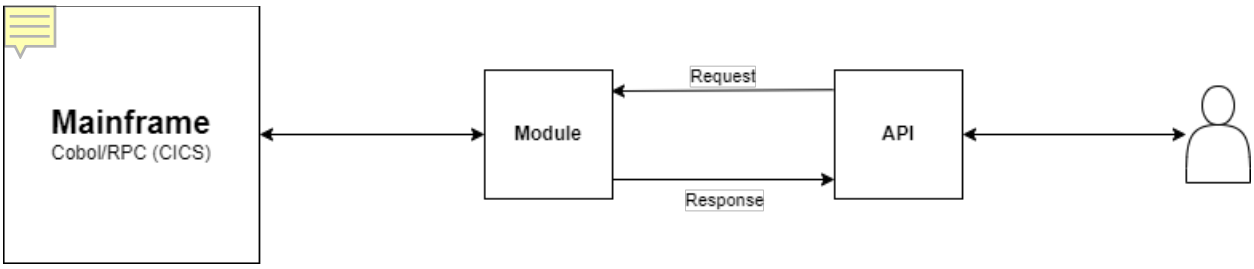

Figure 1: OpenLegacy Reference Architecture for CICS System

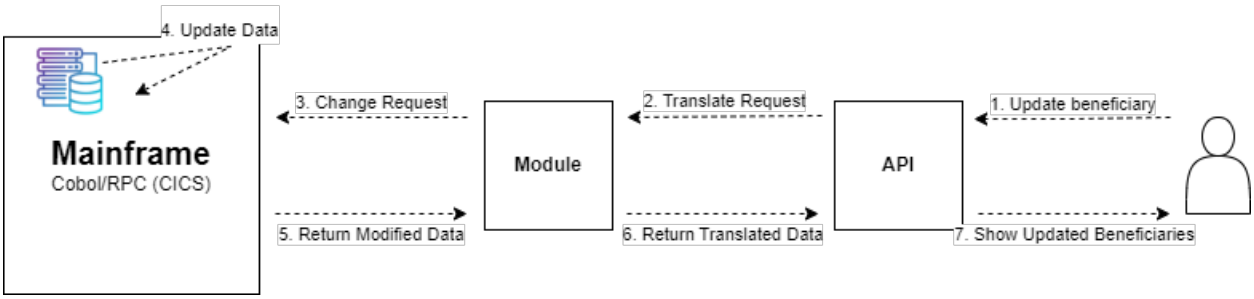

Figure 2: Data Flow through OpenLegacy Microservice (CICS)

Pre-conditions - beneficiary information is already displayed on the mainframe from the database

1. **Update beneficiary** - The user makes a request to modify a beneficiary
2. **Translate request** - The module translates the request from Java data into types the mainframe will understand
3. **Change request** - The mainframe receives the request from the module
4. **Update data** - The beneficiary data is updated in the database
5. **Return Modified Data** - Mainframe returns updated beneficiary data to the module
6. **Return Translated Data** - The module translates the beneficiary data and returns it to the API
7. **Show Updated Beneficiaries** - The API shows the updates to the user

This Beneficiary Data Update Request example demonstrates that all calls go through the microservice (module and API) but no client data is stored within the microservice. It serves as a pipe that translates data and knows how to connect to the legacy system. The system of record and storage is all handled in the DB within the CICS legacy system.

1.6 Detailed OpenLegacy Responses

Following is a breakdown of the specific guidelines for all three standards with OpenLegacy's responses.

GDPR Guideline	Description	OpenLegacy
Do you process EU residents' personal data?	Client Specific Does your company processes, stores or transmits personal data?	Not Applicable to OpenLegacy OpenLegacy does not process, transmit, store or save any personal information related to OpenLegacy clients.

GDPR Guideline	Description	OpenLegacy
	• Basic identity information such as name, address and ID numbers • Web data such as location, IP address, cookie data and RFID tags • Health and genetic data • Biometric data • Racial or ethnic data • Political opinions • Sexual orientation	
Are you a legal entity engaging in Economic Activity	Client Specific	Not Applicable to OpenLegacy
Does your enterprise have less than 250 employees	Client Specific	Not Applicable to OpenLegacy
Right to be forgotten	EU Residents have the right to request to be forgotten and all records will disappear and not be stored anyway	Not Applicable to OpenLegacy The microservices generated by the OpenLegacy platform can help delete the records if so designed, but stores no client data and hence, the regulation doesn't apply.

SOC 2 – Trust Principles	Description	OpenLegacy
Security	Client Specific The security principle refers to protection of system resources against unauthorized access. Access controls help prevent potential system abuse, theft or unauthorized removal of data, misuse of software, and improper alteration or disclosure of information.	Access to OpenLegacy HUB application is permitted only to registered users. For the access control: ● The SaaS offering is using Auth0 ● The on-prem offering is using Keycloak.
Availability	Client Specific The availability principle refers to the accessibility of the client's system, products or services as stipulated by a contract or service level agreement (SLA) to their respective clients, suppliers or vendors.	Not Applicable to OpenLegacy
Processing Integrity	Client Specific The processing integrity principle addresses whether a client system achieves its purpose (i.e., delivers the right data at the right price at the right time). Accordingly, data processing must be complete, valid, accurate, timely and authorized.	Not Applicable to OpenLegacy

SOC 2 – Trust Principles	Description	OpenLegacy
Data Confidentiality	Client Specific Data is considered confidential if its access and disclosure is restricted to a specified set of persons or organizations.	OpenLegacy Hub supports RBAC (Role Based access control)
Privacy	Client Specific The privacy principle addresses the client's system's collection, use, retention, disclosure and disposal of personal information in conformity with an organization's privacy notice, as well as with criteria set forth in the AICPA's generally accepted privacy principles (GAPP).	Not Applicable to OpenLegacy
Storage of client data in SaaS and Cloud vendors	Data stored in Cloud are subject to regulations	OpenLegacy is storing only metadata. The application is GDPR compliant. OpenLegacy's generated microservices do not store client data.
Compliance for SaaS and Cloud Computing Vendors		Although the OpenLegacy Design Time Development Platform has no regulatory or guideline compliance requirements as related to SOC2, we as corporate partners will support and participate, as appropriate

SOC 2 – Trust Principles	Description	OpenLegacy
		to our generated work-product, in any Client driven compliance audits. OpenLegacy participation will include and is not limited to providing scheduled Vulnerability Testing results.

PCI DSS	Description	OpenLegacy
Build and main a secure network	Install and maintain firewall, Don't use vendor supplied passwords, etc	Not Applicable to OpenLegacy OpenLegacy generated microservices reside behind firewalls maintained externally, and does not create or use passwords (handled by CICS and other systems)
Protect Cardholder data	Protect stored data, Encrypt transmission across open networks	Not Applicable to OpenLegacy The OpenLegacy platform enables our clients to incorporate all security and data protection protocols within the Data Message transmission.
Maintain a Vulnerability Management Program	Update anti-virus, maintain secure systems	OpenLegacy conducts annual PT for its application and system vulnerability scanning. End Points - EDR and Antivirus implemented

PCI DSS	Description	OpenLegacy
Implement Strong Access Control Measures	Restrict access, assign a unique ID, restrict physical access	OpenLegacy implemented “Jumpcloud” solution to enable a secure access control
Regularly Monitor and Test Networks		A review and monitoring of the network is carried out periodically
Maintain an Information Security Policy	Maintain a policy that addresses information security for all personnel	There is an information security policy that is communicated to the relevant parties

ISO 27001 Controls	Description	OpenLegacy
A.1-4: Scope & Structure of the standard	The International Standard gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization’s information security risk environment(s).	The company has defined the sections it complies with and the controls it puts in place in order to comply with those sections

ISO 27001 Controls	Description	OpenLegacy
	This standard contains 14 security control clauses collectively containing a total of 35 main security categories and 114 controls.	
A.5: Information security policies	management direction for information security. The objective is to manage direction and support for information security in line with the organization's requirements.	There is an information security policy that is communicated to the relevant parties
A.6: Organization of information security	internal organization and mobile devices and teleworking. The objective is to establish a management framework to initiate and control the implementation and operation of information security within the organization and establish a management framework to ensure the security of teleworking and use of mobile devices	Those responsible for the various areas were defined. There is a policy for managing mobile devices and remote work
A.7: Human resource security	Ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered. Ensure that employees and contractors are aware of and fulfill their information security responsibilities during	Background checks are carried out for candidates, employees receive training in the field of information security. At the time of dismissal, all the privileges granted to the employee during his employment are terminated

ISO 27001 Controls	Description	OpenLegacy
	employment and protect the organization's interests as part of the process of changing and terminating employment.	
A.8: Asset management	Responsibility of assets. identity information assets in scope for the management system and define appropriate protection responsibilities. information classification. Ensure that information receives an appropriate level of protection in accordance with its importance to the organization (and interested parties such as customers). Media handling. Prevent unauthorized disclosure, modification, removal or destruction of information stored on media.	All assets are managed in a central management system. The company's information is classified according to the sensitivity of the information. Use of removable media is carried out in a controlled manner
A.9: Access control	Requirements of access control. limit access to information and information processing facilities. User access management. Ensure users are authorized to access systems and services as well as prevent unauthorized access. User responsibilities. Make users accountable for safeguarding their	Access control to the various systems based on the need to know & least privilege principle Access to the various systems via a complex password +2FA, as well as automatic locking after a period of non-use All employees sign information security rules

ISO 27001 Controls	Description	OpenLegacy
	authentication information. System and application access control. Prevent unauthorized access to systems and applications.	
A.10: Cryptography	Cryptographic controls. Ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.	Use of HTTPS encrypted communication. Laptops are encrypted using the ESET system. Databases in the SAAS service are encrypted
A.11: Physical and environmental security	Ensuring secure physical and environmental areas. Prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities. Equipment. Prevent loss, damage and theft or compromise of assets and interruption to the organization's operations.	Use of cloud systems only. There are no physical servers in the organization Employees sign rules for using and maintaining the personal computer.
A.12: Operations security	Operational procedures and responsibilities. Protection from malware. Backup. Logging and monitoring. Control of operational software. Technical vulnerability management. Information systems and audit considerations.	Anti-virus software is installed on all computers. There are backups of the sensitive information, as well as logs collected from central systems. A vulnerability scan and penetration test is performed once a year

ISO 27001 Controls	Description	OpenLegacy
A.13: Communications security	Network security management. Protection of information in networks and its supporting information processing facilities. Information transfer. Maintain the security of information transferred within the organization and with any external entity, e.g. a customer, supplier or other interested party.	Connection to cloud environments is done in an encrypted way. There is a separation of networks: an internal network and a guest network
A.14: System acquisition, development and maintenance	Security requirements of information systems. Ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.	The development environments are separated. The employees undergo training at SSDLC There is a tool for scanning vulnerabilities in the code. A QA test is performed before uploading to production
A.15: Supplier relationships	Information security in supplier relationships. Protection of the organization's valuable assets that are accessible to or affected by suppliers. Supplier service development management. Ensure that an agreed level of information security and service delivery is maintained in line with supplier agreements.	Suppliers sign an information security annex, and regular reviews are carried out on suppliers who have access to information.

ISO 27001 Controls	Description	OpenLegacy
A.16: Information security incident management	Management of information security incidents, events, and weaknesses. Ensure a consistent and effective approach to the lifecycle of incidents, events and weaknesses.	There is a plan for handling information security incidents, the plan is practiced.
A.17: Information security aspects of business continuity management	Information security continuity. Information security continuity shall be embedded in the organization's business continuity management systems. and ensure availability of information processing facilities.	There is a disaster recovery plan, the plan is practiced. (use of cloud systems)
A.18: Compliance	compliance with legal and contractual requirements. Avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.	The company has identified the laws and regulations to which it is subject. An information security review is performed once a year as part of the ISO27001 certification

Summary

OpenLegacy truly appreciates the importance of adhering and supporting GDPR, SOC2 and PCI compliance guidelines. As a Design Time Development platform that does not store or persist any customer, personal, or confidential data, the terms and conditions of compliance do not apply to the OpenLegacy Platform, but can apply to our clients' generated API and Microservices (platform work product).

However, as good corporate partners, OpenLegacy is committed to support and participate as appropriate in client-driven compliance audits, including, but not limited to providing scheduled Vulnerability Testing results.

For any questions or queries related to Data Security Compliance, please contact OpenLegacy at:

Cs.sales@openlegacy.com