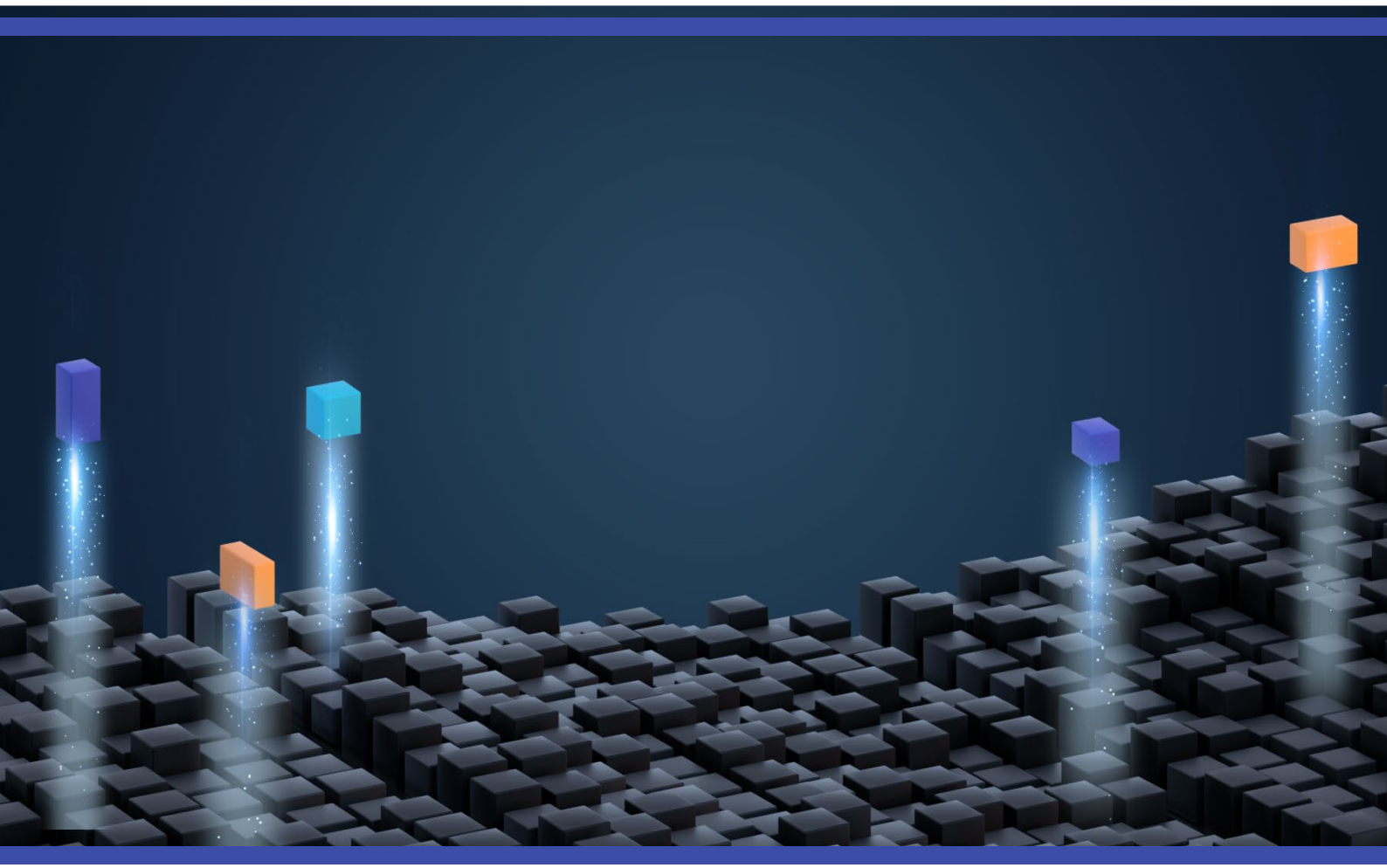
OpenLegacy
Digital to the Core

OpenLegacy Data Security

POSITION PAPER

March 2021



Contents

1 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.

2 Compliance Definitions

2.1 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.

2.2 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.

2.3 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.

3 OpenLegacy Compliance

3.1 Reference Architecture Example - CICS

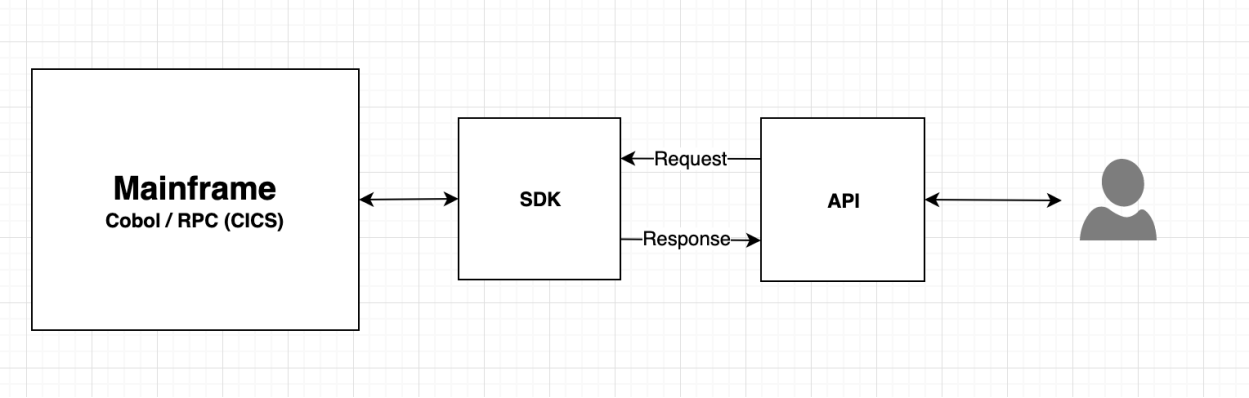


Figure 1: OpenLegacy Reference Architecture for CICS System

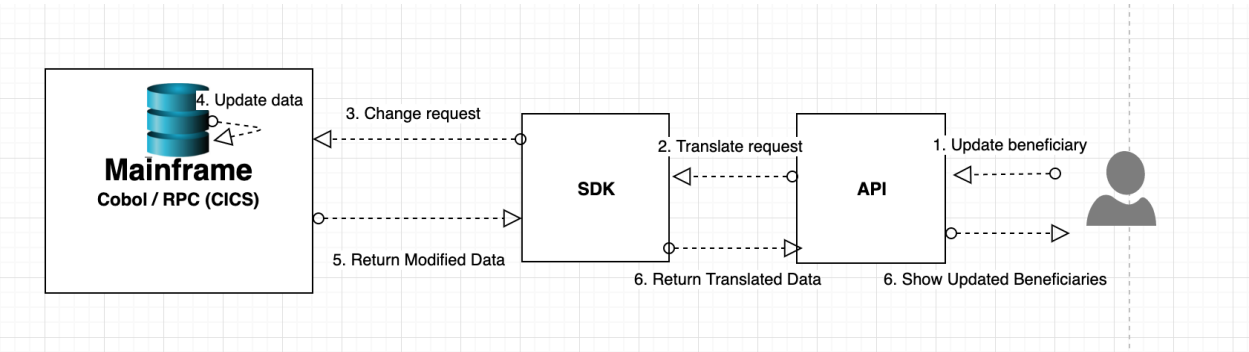


Figure 2: Data Flow through OpenLegacy Microservice (CICS)

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 SDK translates the request from Java data into types the mainframe will understand
3. **Change request** - The mainframe receives the request from the SDK
4. **Update data** - The beneficiary data is updated in the database
5. **Return Modified Data** - Mainframe returns updated beneficiary data to the SDK
6. **Return Translated Data** - The SDK 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 (SDK 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.

3.2 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? • 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	Not Applicable to OpenLegacy The OpenLegacy platform is a design time development platform, focused on providing our clients with integration capabilities between their systems of record (internal) and systems of engagement (external). Within the OpenLegacy platform, the templating feature and the developer IDE enable the client to apply and incorporate their respective compliance needs in the OpenLegacy Client Owned Work-Product (API / Microservice). It is the client's responsibility to define, apply and accommodate their respective regulatory requirements as related to GDPR. Usage and deployment of the OpenLegacy platform is the responsibility of the client. An industry best practice when related to Integration – is to not persist or store any data that is being delivered (Message). The OpenLegacy Platform does not contain any out of the box capability

GDPR Guideline	Description	OpenLegacy
		to Persist or Store Message/Transaction data.
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.	OpenLegacy as a Design Time Development Platform is fully capable of incorporating our client's security requirements. This incorporation is performed by our clients using our templating or developer IDE. Our clients have successfully incorporated the following security protocols and capabilities into their respective OpenLegacy generated APIs &

SOC 2 – Trust Principles	Description	OpenLegacy
		Microservices (Work Products). • Oauth2 • Mainframe Security (RACF, ACF2, etc.) • WAFs • Two factor authentications • Token authentication • Intrusion detection • Encryption
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
Data Confidentiality	Client Specific Data is considered confidential if its access and	Not Applicable to OpenLegacy

SOC 2 – Trust Principles	Description	OpenLegacy
	disclosure is restricted to a specified set of persons or organizations.	
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	Not Applicable to OpenLegacy 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 to our generated work-product, in any Client driven compliance audits. OpenLegacy participation will include and is not limited to

SOC 2 – Trust Principles	Description	OpenLegacy
		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	Not Applicable to OpenLegacy
Implement Strong Access Control Measures	Restrict access, Assign a unique ID, restrict physical access	Not Applicable to OpenLegacy The OpenLegacy platform enables our clients to incorporate all access security, access logging and control, and data protection protocols .
Regularly Monitor and Test Networks		Not Applicable to OpenLegacy

PCI DSS	Description	OpenLegacy
Maintain an Information Security Policy	Maintain a policy that addresses information security for all personnel	Not Applicable to OpenLegacy

4 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