

CUSTOMER — SUCCESS STORY

SISA Evaluates Privacy Risks across Fintech Firm's Applications

ABOUT THE CUSTOMER

The client, a leading digital payment solutions provider headquartered in Mumbai, specializes in bridging the gap between physical and digital payments across India. Established in April 2018, the company connects thousands of agents—such as kirana shops, pharmacies, and mom-and-pop stores—to the formal banking system, enabling consumers nationwide to access digital financial services. The client also serves as a technology partner for a leading Indian bank, developing critical applications to process and handle sensitive financial data on behalf of such banks.

THE BUSINESS REQUIREMENT

The client handles vast volumes of Personally Identifiable Information (PII) on behalf of their customer through critical applications. They faced an urgent need to conduct a Data Protection Impact Assessment (DPIA). This assessment would evaluate privacy risks and their current privacy posture and maturity. It would also demonstrate the adequacy of privacy controls in place for their critical applications. With the enactment of the Indian Digital Personal Data Protection Act (DPDPA) 2023, non-compliance could lead to financial penalties, operational disruptions, and reputational risks, jeopardizing their relationships with key stakeholders. Classified as a Data Fiduciary and a Data Processor under the DPDPA, the client needed to perform a DPIA to identify, assess, and mitigate risks associated with the core applications that they provide to their Significant Data Fiduciary. To ensure seamless adherence to legal mandates while fortifying their data protection framework, they sought a trusted cybersecurity partner with expertise in regulatory compliance, risk assessment, and privacy-driven security solutions.

THE SOLUTION

The client chose SISA to perform a Data Protection Impact Assessment for the corresponding critical applications. To gain insights into the organizations current data privacy practices and controls implemented by the data processor within these applications, the assessment was conducted through a combination of applications demos, study of existing processes, documents through walkthroughs, workshops and questionnaires. The questionnaires included an in-depth assessment of the following in all processes of the applications:



Transparency

This aspect focused on evaluating whether the application's privacy notice was sufficiently clear and informative for users. The objective was to determine if users were adequately informed about how their data is collected, processed, and stored within the application.



Data Collection and Usage

Conducted a comprehensive assessment of the personally identifiable information (PII) collected, processed, and utilized by each application. The review focused on ensuring compliance with data privacy regulations and alignment with business objectives.



Data Storage and Retention

Evaluated data storage architecture, retention policies, and storage locations to ensure compliance with regulatory requirements and industry best practices. Assessed the duration for which data is retained and the effectiveness of data minimization strategies.



Data Sharing and Integrations

Analysed data flows between applications, including API integrations and external data transfers. Assessed third-party data processing activities and the adequacy of contractual agreements governing data protection and compliance obligations.



Access Controls and Safeguards

Reviewed the implementation of identity and access management (IAM) controls, authentication mechanisms, and security safeguards to mitigate risks associated with unauthorized access, data breaches, and insider threats.



Data Security in Transmission

Analysis of measures to secure data during transmission and sharing with external parties.



Consent Management practices

Evaluated the effectiveness of consent management frameworks, including mechanisms for obtaining, tracking, and managing user consent in accordance with global privacy regulations. Assessed the transparency and granularity of consent options provided to users.

Finally, SISA's team also reviewed internal audits and assessments conducted by the client's team.

SISA's evaluation highlighted several key risks and areas for improvement:



Deficient Inventory of Data Processing Activities

The client lacked a comprehensive and up-to-date inventory of data processing activities, making it difficult to track how personal data is handled across applications and business units. To address this, it was recommended to develop and maintain a structured inventory of processing activities, ensuring clear visibility and control over personal data handling.



Lack of Defined Processes for DSARs

The absence of well-defined processes for handling DSARs resulted in risks of delays, confusion, or even non-compliance with privacy regulations. To address this, the client was advised to define and document standardized procedures for handling DSARs, ensuring timely and accurate responses to data access requests while maintaining regulatory compliance.



Absence of Clearly Defined Data Retention Policies

The absence of clear data retention policies posed risks such as retaining personal data longer than necessary, increasing exposure to breaches and non-compliance with privacy regulations. To mitigate this, the organization was advised to establish well-defined data retention policies with specific retention periods, reducing the risk of over-retention and regulatory violations.



Inconsistent Communication of Privacy Notice Updates

Privacy notice updates were not consistently communicated to employees and customers, undermining transparency, trust, and stakeholders' understanding of data usage and protection. To improve this, SISA recommended implement a structured mechanism for notifying Data Principals of updates to privacy notices, ensuring informed data handling practices and reinforcing trust.



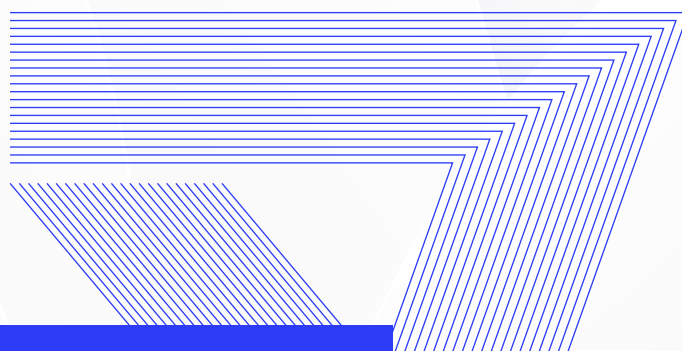
Absence of a Formal Consent Withdrawal Mechanism

The organization lacked a clear process for individuals to withdraw consent for data processing, which could lead to unauthorized or non-compliant data use. To resolve this, it was recommended to integrate a structured mechanism for consent withdrawal within the Data Subject Access Request (DSAR) process, ensuring compliance with regulatory requirements and respecting data subject rights.

BUSINESS IMPACT

Addressing these gaps not only improved their existing privacy practices but also helped build stronger relationships with their customers, fostering trust and accountability.

The DPIA significantly enhanced the bank's visibility into its data processor's privacy practices, ensuring compliance with regulatory requirements and industry standards, reinforcing the established business relationship with the bank and significantly reducing the risk of non-compliance. The DPIA improved operational efficiency, minimizing risks associated with data over-retention and unauthorized processing. The assessment also enhanced responsiveness to regulatory and customer requests, fostering greater transparency and trust. By mitigating key risks, the assessment positioned the data processor as a reliable and compliant entity, enhancing its reputation and competitive standing. Ultimately, the exercise not only ensured adherence to privacy regulations but also provided a framework for sustainable data protection, enabling long-term resilience and trust.



ABOUT SISA

SISA is a Global Leader in Cybersecurity Solutions for the Digital Payment Industry. As a Global Payment Forensic Investigator of the PCI Security Standards Council, we leverage forensics insights into preventive, detective, and corrective security solutions, protecting 1,000+ organizations across 40+ countries from evolving cyberthreats. Our suite of solutions from AI-driven compliance, advanced security testing, agentic detection/ response and learner focused-training has been honored with prestigious awards, including from Financial Express, DSCI-NASSCOM and The Economic Times. With commitment to innovation, and pioneering advancements in Quantum Security, Hardware Security, and Cybersecurity for AI, SISA is shaping the future of cybersecurity through cutting-edge forensics research.

Compliance	Security Testing	Cyber Defense	Data Protection & Governance	Trainings & Certifications	Leading Tech Security
Payment Data Security • PCI DSS • PCI PIN • PCI 3DS • PCI P2PE • PCI S3 • PCI S-SLC • PCI CP (Card Production) • Facilitated PCI SAQ • Quarterly Health Check-ups • Central Bank Compliance • SWIFT Strategy and Risk • CCPA • GDPR • HIPAA • ISO • NIST • SOC 1 • SOC 2 • Cloud Security • HITRUST Unified Audits Managed Compliance	Application Security • Application Penetration Testing • CREST/CERT-in Approved Security Testing • API Security Testing • Secure Code Review Network Security • Vulnerability Assessment • Penetration Testing • Configuration Review • Firewall Rule Review • PCI ASV Scan Phishing Simulation Red Teaming Exercise • Layer Security Testing	Managed Extended Detection and Response Solution - SISA ProACT • 24x7 Monitoring • UEBA • Threat Intel • Advanced Threat Hunting • Breach & Attack Simulation • SOAR • Use-case Factory Digital Forensics and Incident Response • Incident Response / Compromise Assessment Services • Forensic Readiness Audit • Forensic and Incident Response Retainer Service • PCI Forensic Investigation (PCI) • Internal Forensic Investigation (IFI) • Ransomware Simulation	Data Discovery and Classification • PCI/PII/PHI Data Discovery • Data Classification in Endpoint (Windows, Linux) • Data Classification in O365, Metadata • Dynamic Masking, Redact, Truncation • Integration to DRM, DLP, SIEM Data Privacy Professional Services • Assessments (Unified Privacy Maturity, DPIA, 3rd Party Risk) • Data Inventory, Mapping and Process flow, RoPA • Data Privacy Framework - Policy, Notice, SoPs • Consent and Notice Management framework • Data Breach and Management • Principal management • Privacy by Design implementation guide • Define Data Retention Guidelines and processes • Technical/Organization measures • Privacy Training/Awareness	Payment Data Security Training and ANSI Accredited Certification • CPISI (2 Day Program) • CPISI (3 Day Program) • CPISI- Advanced (3 Day Program) • CPISI-D (Developers) • CPISI Hybrid (4 Weeks) Certification Program in Cybersecurity for AI – CSPAI • CSPAI Forensic Briefing Sessions for Senior Management	AI PRISM • AI PRISM LLM Vulnerability Scanner Solution • AI Risk Management and Governance Solution Framework • AI Compliance and Governance Consulting Service Hardware and IoT Security Testing • Firmware Security Testing • Hardware/Embedded Security Testing • IoT Network Security Testing • IoT/Embedded Application and Management Layer Security Testing • MPOC/ PCI PTS Quantum Security • Quantum Cryptographic Consulting • Quantum Security Risk Assessment • Quantum Security Standards Compliance

SISA is a Global Leader in Cybersecurity Solutions for the Digital Payment Industry

USA | Canada | UK | Bahrain | Saudi Arabia | UAE | Qatar | India | Singapore | Malaysia | Australia

To learn more about SISA's offerings visit us at www.sisainfosec.com or
Contact your SISA sales representative at contact@sisainfosec.com