

Kiteworks Supports the Bahamas Data Protection Act, 2025

Data Sovereignty, Possessionless Editing, and Real-Time SIEM Feeds Operationalize the Bahamas' Modernized Privacy Framework

Solution Highlights



Strong Double Encryption



Data Sovereignty and Geofencing



ABAC Data Policies



SafeEDIT Possessionless Editing



Secure Data Forms



Comprehensive Audit Logs With SIEM Feeds

The Data Protection Act, 2025 is a comprehensive privacy statute enacted by the Parliament of The Bahamas, with commencement dates to be set by the Minister via Gazette notice. It repeals the prior Data Protection (Privacy of Personal Information) Act and applies to all data controllers and processors, public and private, operating in The Bahamas or processing the personal data of Bahamian data subjects from abroad. The Act covers every sector without industry restriction and carries meaningful teeth: violations of core data protection principles, unauthorized disclosure, and noncompliance with enforcement notices each carry summary-conviction fines up to fifty thousand dollars and imprisonment up to three years (Sections 4, 47, 80, and 96), while the Commissioner can also issue civil penalty notices under Section 90 enforceable as Supreme Court judgments. Kiteworks supports organizations working toward compliance with the Data Protection Act, 2025. Here's how:

Technical Safeguards Across Processing (Sections 11 and 53)

Sections 11 and 53 require technical and organizational measures proportionate to processing risk, disclosed to data subjects, and reviewed on an ongoing basis, while Section 47 prohibits unauthorized disclosure of personal data. Kiteworks deploys as a hardened virtual appliance that minimizes attack surface, layering file and disk double encryption with TLS 1.3 in transit, AES-256 by default, and optional FIPS 140-3 validation. Attribute-based access controls, called Data Policies within Kiteworks, enforce non-disclosure obligations dynamically across data, user, and action attributes, routing sensitive files into SafeEDIT or SafeVIEW so they never leave the Kiteworks environment. A Data Loss Prevention integration and built-in F-Secure antivirus scanning, including on files passing through the Email Protection Gateway, screen for malware on both upload and download. Risky Settings Detection gives administrators a continuous review mechanism aligned with the periodic-review obligations these sections impose, displaying alerts upon admin login when risky settings are detected and sending periodic email alerts.

Data Subject Rights Across Sections 5 Through 56

Data subject rights spanning accuracy, erasure, consent, restriction, portability, and cross-border transfer sit throughout Part IV and Section 50, with Section 8 setting the transparency-at-collection baseline and Section 54 governing transfers outside The Bahamas. Secure Data Forms meet that transparency and consent-evidence standard, generating a human-readable PDF and machine-readable CSV per submission. Legal and admin file withdrawal, paired with the Withdrawal feature, fulfills erasure and access-revocation obligations, while ABAC Data Policies and Legal hold and eDiscovery controls address processing restrictions. Portability is served by CSV, JSON, and XML export plus the Kiteworks REST API and direct vault-to-vault transfers between Kiteworks deployments. Automated decision-making restrictions are enforced through ABAC together with the Kiteworks Secure MCP Server, which confines AI operations to the acting user's own permissions. Data sovereignty and geofencing enforce cross-border transfer limits, restricting access by blocked country or IP address. Registration, DPO appointment, Commissioner notifications, and appeal procedures remain the organization's direct responsibility.

Seventy-Two-Hour Breach Detection and Section 44 Processing Records

Sections 44 and 48 require structured processing records and breach detection and notification within seventy-two hours, with Sections 45 and 51 adding audit and impact-assessment obligations. Comprehensive audit logs with SIEM feeds form the backbone here, normalizing and streaming log data in real time to systems including QRadar, LogRhythm, ArcSight, and Splunk so the notification clock starts the moment AI-based intrusion and anomaly detection flags suspicious activity. Log timeliness appends entries immediately, with no batching delay, and trusted audit logs convert that data into human-readable, filterable reports for compliance audits. Compliance summary reports, covering Audit Log, CMMC 2.0, Insider Threats, Outsider Threats, GDPR, and HIPAA, satisfy Section 44's processing-record requirement, while data sovereignty reporting and geofencing document transfer destinations and retention safeguards for offshore-server audits. The Risk Policy Audit Log Report and Risky Settings Detection together keep Section 51's impact assessments and periodic security reviews current rather than point-in-time exercises.

Kiteworks addresses the Data Protection Act, 2025's technical safeguard obligations through a hardened virtual appliance, file and disk double encryption, and DLP integration, giving data controllers and processors the layered security posture that Sections 11 and 53 demand. Data subject rights across accuracy, erasure, portability, consent management, and cross-border transfer restrictions are operationalized through Secure Data Forms, ABAC Data Policies, the Withdrawal feature, vault-to-vault MFT Server transfers, and data sovereignty and geofencing controls that enforce jurisdictional limits at the user, profile, and system level. The Act's breach detection, processing records, and periodic review obligations are sustained by real-time SIEM-fed audit logs, AI-based intrusion detection, trusted audit logs, and Risky Settings Detection, which together keep the seventy-two-hour notification window practical and Commissioner-directed reviews current. Kiteworks brings all three domains together in a single platform, providing data controllers and processors with a unified technical foundation for ongoing Data Protection Act, 2025 compliance.

Ready to see how Kiteworks supports Data Protection Act, 2025 compliance?

www.kiteworks.com

Kiteworks



Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and use of private data. The Kiteworks platform provides customers with a secure data exchange that delivers data governance, compliance, and protection in a unified control plane. Kiteworks unifies, tracks, controls, and secures sensitive data moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all private data exchanges. Headquartered in Silicon Valley, Kiteworks protects over 100 million end-users and thousands of global enterprises and government agencies.