Kiteworks

COMPLIANCE BRIEF

From Exposure to Compliance: Support for Israel's Privacy Protection Law With Kiteworks

How Organizations Can Close the Gap on Security and Monitoring Requirements

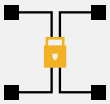
Israel's Protection of Privacy Law (5741-1981), as modernized by Amendment No. 13 (effective August 14, 2025), applies broadly to any organization or individual that infringes upon personal privacy—covering everything from surveillance and unauthorized use of personal likeness to electronic data processing—though its most detailed compliance obligations, including data security requirements, subject rights, and administrative enforcement, focus specifically on organizations that maintain databases containing personal data of Israeli residents. Organizations were to achieve compliance by August 2025, one year from the law's publication date, with certain provisions for Israel Police databases taking effect three years after commencement. Noncompliant organizations face administrative fines from the Israeli Privacy Protection Authority (PPA) of up to NIS 320,000 per violation, with fines potentially doubling to NIS 640,000 in aggravated cases involving sensitive data or large-scale databases, and total penalties that may exceed these caps when scaled by number of affected individuals or duration of noncompliance. Kiteworks helps organizations meet these requirements through its Private Data Network (PDN). Here's how:

Data Security and Technical Safeguards

Israel's Privacy Protection Law places direct responsibility on database controllers and holders to secure personal data in their systems. Section 17(a) establishes that both parties bear independent security obligations, while Section 17(b) authorizes regulations covering physical and logical database protection, work procedures, and restrictions on employee data access. Organizations processing information of special sensitivity face heightened exposure to financial sanctions for security failures. Kiteworks addresses these requirements through multiple layered security controls. The platform deploys as a hardened virtual appliance that minimizes the attack surface through an embedded network firewall and an embedded web application firewall, blocking unauthorized access at the perimeter. Kiteworks encrypts customer files at rest and applies TLS 1.3 for all data in transit. The single-tenant private cloud architecture ensures no database, file system, or application runtime sharing with other customers, directly supporting the law's mandate for rigorous data protection.

Solution Highlights

Hardened virtual appliance



Strong double encryption

Single-tenant private cloud architecture

Comprehensive audit logging with SIEM feeds

Customizable administrative roles and separation of duties

Data Processing Controls and Access Governance

The law establishes comprehensive controls over how organizations process personal data in their databases. Sections 8(b) and 8(c) require processing to occur only for lawfully determined database purposes and only with controller authorization. Section 11 requires organizations to notify data subjects of their obligations, data use purposes, and rights before collecting personal data. Sections 13 and 14 grant data subjects rights to review and correct their personal information, and controllers must respond within regulation-specified timelines. Kiteworks supports these control requirements through its access control and identity management capabilities. The platform integrates with external identity management systems including LDAP and Microsoft Active Directory, and applies access control policies across all data folders, emails, and connections. Kiteworks implements the principle of least privilege, granting users no default privileges and expanding access only as administrators specify for defined roles, ensuring personal data flows only to authorized parties within sanctioned processing purposes.

Compliance Monitoring and Audit Logging

Section 17B1(a)(3) requires database controllers and holders whose activities involve regular and systematic monitoring of individuals on a significant scale to appoint a Data Protection Officer. Section 17B2(a)(2) requires that officer to prepare and implement an ongoing compliance monitoring program, report findings to management, and propose corrective measures. These requirements demand that organizations maintain detailed records of data processing activities and demonstrate active oversight to the Privacy Protection Authority. Kiteworks supports these tracking obligations through its comprehensive audit logging capabilities. The platform automatically collects, cleans, normalizes, standardizes, and aggregates security and compliance activity data into a single log stream that feeds directly into SIEM systems. Administrators access tracking data based on customizable admin roles, enforcing administrative separation of duties. Kiteworks also generates compliance summary reports that demonstrate adherence to specific policy controls, giving Data Protection Officers documented evidence of ongoing monitoring required under the law.

Kiteworks provides organizations subject to Israel's Privacy Protection Law (Amendment No. 13) with an integrated platform that addresses the regulation's three core compliance domains through a unified architecture. By combining technical safeguards with granular access governance and continuous monitoring capabilities, Kiteworks enables controllers and holders to meet their independent obligations under the law without relying on disparate tools. This means organizations can demonstrate to the Privacy Protection Authority that they maintain appropriate security controls, enforce purpose-limited data processing, and generate the documented evidence that Data Protection Officers require to fulfill their statutory monitoring and reporting duties. Kiteworks' single-tenant design, layered security architecture, and comprehensive audit infrastructure collectively position organizations to address regulatory requirements across all enforcement tiers the law establishes.