Kiteworks

COMPLIANCE BRIEF

Support for the German Data Protection Act Requirements

Secure Data Communications for BDSG Requirements

The German Federal Data Protection Act (BDSG) implements the EU's General Data Protection Regulation (GDPR) with specific national provisions for Germany. Enacted in 2018, the BDSG applies to all organizations processing personal data within German territory, including public bodies, healthcare providers, financial institutions, and businesses across all sectors. The law establishes strict requirements for handling sensitive information, particularly special categories of personal data like health records and political opinions. Organizations must comply immediately with these regulations, as noncompliance carries significant consequences—fines can reach up to €20 million or 4% of global annual revenue, whichever is higher. Companies also face potential legal action from affected individuals, regulatory investigations, and reputational damage. Kiteworks offers a comprehensive private data exchange platform that addresses multiple BDSG compliance requirements through robust security controls, detailed audit capabilities, and streamlined data protection management.

BDSG Special Categories Protection Through Kiteworks Zero-trust Data Exchanges

The BDSG establishes strict controls for processing special categories of personal data, including health information. The Act permits such processing only for specific purposes, such as preventive medicine, healthcare provision, or when public bodies must prevent substantial threats to public security. The law requires controllers to implement appropriate safeguards for data subjects' rights when processing sensitive information. Kiteworks addresses these requirements through its comprehensive attribute-based access controls (ABACs), which enable administrators to define and enforce dynamic policies based on data attributes, user profiles, and specific actions. For medical data processing, Kiteworks implements role-based access controls (RBACs) to ensure only authorized health professionals access sensitive information. The system's hardened virtual appliance architecture with double encryption protects confidentiality, while comprehensive audit logs maintain detailed records of all health data processing to demonstrate compliance with professional secrecy requirements.

Solution Highlights

- Zero-trust data exchanges
- Comprehensive audit logs
- Hardened virtual appliance
- Double encryption
- Least-privilege defaults
- SIEM integration

Safeguards Maintained With Multi-factor Authentication and Risk Detection

Section 22(2) requires organizations to implement specific safeguards when processing special categories of personal data, taking into account technical state of the art, implementation costs, and processing risks. These measures must protect data subjects' interests while ensuring appropriate security based on risk assessment. Kiteworks delivers a robust security framework that directly addresses these requirements through multiple protective layers. The platform offers comprehensive authentication methods including multi-factor authentication supporting RADIUS protocol, PIV/CAC cards, and multiple one-time password options (email-based, SMS-based, and time-based RFC 6238 standard). Access control is enforced through granular RBAC and ABAC permissions with least-privilege defaults, while location-based restrictions like geofencing and IP address filtering provide additional protection. Kiteworks implements zero-trust data exchanges aligned with industry standards such as NIST CSF, and includes automatic detection of risky configuration changes through its "Risky Settings" dashboard, which requires authorization sign-off before allowing potentially dangerous changes. This proactive approach supports continuous compliance with GDPR and BDSG security requirements.

Tracking Requirements Supported by Comprehensive Audit Logs

The tracking requirements in the BDSG mandate robust auditing and record-keeping for all data processing activities. Sections 22(2), 62(5), 64(3), and 70 require organizations to implement measures that verify who accessed, modified, or removed personal data, maintain detailed processing records, track data transfers, and make these records available to authorities. These provisions ensure accountability and transparency in data processing operations. Kiteworks addresses these requirements through its comprehensive audit logs with SIEM integration, which capture detailed information about all system activities. The platform logs every action on data—including file edits, uploads, deletions, and sharing—recording the user ID, filename, time stamp, and location for each operation. Kiteworks offers dedicated auditor roles with access to the reports portal in the compliance console and provides exportable audit logs via syslog or Splunk Universal Forwarder. The system generates activity reports documenting all logged activities and usage reports for tracking processing operations, supporting both controller record-keeping obligations and regulatory inspections by the Federal Commissioner.

Kiteworks provides a comprehensive solution for organizations needing to comply with the German Federal Data Protection Act. The platform's ABACs enable granular control over special categories of personal data by restricting access and actions based on data sensitivity, user roles, and processing purpose. Organizations can maintain compliance through robust security safeguards including multi-factor authentication, RBACs, and encryption at rest and in transit. These technical measures directly address the law's risk-based security requirements while protecting data subjects' rights. Comprehensive audit logs capture complete records of all data interactions, supporting the accountability and transparency mandated by the regulation. With dedicated compliance reporting, automatic risky settings detection, and specialized features for healthcare data protection, Kiteworks helps organizations avoid substantial penalties while maintaining operational efficiency. The platform transforms BDSG compliance from a challenging obligation into a streamlined, integrated part of secure data management practices.

Kiteworks

April 2025

www.kiteworks.com