Solution Brief

Preparing for Compliance with Saudi Arabia's PDPL

Netskope's comprehensive cybersecurity and data protection solutions are designed to help organizations in the Kingdom of Saudi Arabia meet the stringent requirements of the SDAIA Personal Data Protection Law (PDPL). With advanced capabilities to protect data, ensure data residency, and support regulatory compliance, Netskope empowers organizations to safeguard sensitive personal data and mitigate the risks associated with non-compliance.

Quick Glance

How Netskope Supports PDPL Compliance

- Netskope empowers organizations to meet the Kingdom of Saudi Arabia's high standards for personal data protection, including data residency, breach management, and cross-border data controls.
- Real-time data monitoring and advanced DLP safeguard sensitive data, providing robust protection against unauthorized access and enabling rapid breach detection.
- Automated record-keeping, reporting, and data classification simplify regulatory adherence, making compliance management efficient and transparent.
- Comprehensive risk assessments, visibility into data transfers, and advanced analytics support strong data governance and reduce compliance risks.

Introduction

The Saudi Authority for Data and Artificial Intelligence Act (SDAIA) has introduced comprehensive regulations under the Personal Data Protection Law (PDPL) and its related frameworks, fundamentally reshaping the data protection landscape in the Kingdom of Saudi Arabia. The PDPL is modeled after the GDPR and establishes strict rules for the collection, processing, and protection of personal data. Organizations processing personal data within Saudi Arabia, or those processing data of Saudi residents, must adhere to these regulations to safeguard sensitive information, enhance transparency, and ensure accountability. Compliance is essential for maintaining trust and avoiding significant penalties.

Scope of the SDAIA PDPL

The PDPL governs any processing of personal data related to individuals that takes place within Saudi Arabia, regardless of the methods or technologies used, and extends to entities outside the Kingdom if they handle the personal data of individuals residing in Saudi Arabia. It applies to both general and sensitive personal data, such as health and genetic information, offering specific protections. Exemptions are provided for data processed for personal or family use, as long as the data is not disclosed or published. The law also uniquely includes the personal data of deceased individuals if that information can identify them or their relatives, ensuring broad protection of private information.

Challenges for Data Protection

Complying with the PDPL poses significant data protection challenges for organizations.

Key issues include:

1. **Data breach management**: Organizations must ensure they have the capability to identify and report data breaches swiftly. The PDPL requires controllers to notify the SDAIA of any breaches within a 72-hour time frame, ensuring transparency and swift remediation.
2. **International data transfers**: The PDPL places stringent restrictions on the transfer of personal data outside Saudi Arabia. Without clear adequacy decisions or proper safeguards, businesses face complexities in ensuring compliant cross-border data transfers, making it essential to adopt robust data residency solutions.
3. **Sensitive data protection**: The law requires organizations to implement rigorous security controls to protect sensitive personal data, including health, genetic, and biometric information.
4. **Record-keeping and accountability**: Organizations must maintain accurate records of data processing activities, particularly for high-risk processing that requires Data Protection Impact Assessments (DPIAs). Failure to document and demonstrate compliance can lead to penalties.

By addressing these challenges and implementing strong data protection measures, businesses can not only ensure compliance with the PDPL but also enhance their overall data governance and security posture.

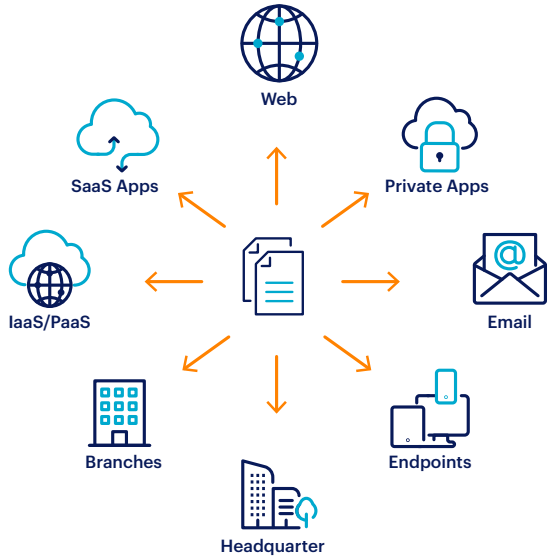
Solving Data Protection Challenges with Netskope

Netskope provides comprehensive solutions to help organizations comply with the Personal Data Protection Law (PDPL) in Saudi Arabia. Through the Netskope One Secure Access Service Edge (SASE) platform's advanced technical controls, Netskope enables data protection, visibility, risk management, and incident response, ensuring that businesses can securely manage and process personal data while meeting regulatory requirements.

Netskope One highlights for personal data protection:

- **Data residency**: Netskope's global infrastructure with data centers in Saudi Arabia ensures personal data remains within the Kingdom, or specific geographic regions, meeting the PDPL's cross-border data transfer restrictions.
- **Data protection**: Netskope One Data Loss Prevention (DLP) and encryption is performed in Saudi Arabia and ensures sensitive data is protected both in transit and at rest.
- **Visibility and control**: Real-time cloud activity monitoring and user and entity behavior analytics (UEBA) help detect suspicious activities and ensure data compliance.
- **Risk management**: Risk assessments and compliance reporting provide detailed insights and audit trails to support regulatory compliance.
- **Incident response**: Automated threat protection and incident response streamline compliance with the PDPL's 72-hour breach notification requirement.

Fig 1: Netskope Comprehensive Data and SaaS Security



Proactive Data Breach Prevention and Swift Incident Response

Data breaches are a critical threat to an organization's reputation and legal standing, especially under the PDPL, which mandates swift reporting within a 72-hour window. Netskope One Cloud Access Security Broker (CASB) and Netskope One Next-Gen Secure Web Gateway (NG-SWG) utilize the Netskope One DLP engine to identify, monitor, and secure personal data across various environments, such as web, cloud applications, and endpoint devices. This capability ensures that personal data is actively protected from unauthorized access, reducing the risk of breaches and ensuring compliance with breach notification requirements.

Highlights of Netskope One DLP include:

- **Real-time breach detection**: The Netskope One DLP engine continuously scans and monitors personal data across diverse environments, enabling real-time identification of potential breaches and reducing the risk of data exposure.
- **Swift response and remediation**: Leveraging machine learning and advanced analytics, Netskope provides visibility into data flows and breach points, ensuring timely remediation and minimizing the impact of breaches.
- **Compliance with notification requirements**: Detailed forensic reporting assists in meeting the PDPL's 72-hour breach notification requirement by providing insights into the scope and impact of the breach.

Netskope's real-time detection and response capabilities ensure organizations can proactively manage data breaches, protect sensitive information, and meet regulatory deadlines.

Ensuring Secure and Compliant Cross-Border Data Transfers

The PDPL enforces strict limitations on cross-border data transfers, presenting challenges for organizations that operate either in neighboring countries, regions, or globally. The Netskope One DLP engine and Cloud Confidence Index (CCI) enable organizations to monitor, control, and secure personal data transfers in accordance with the PDPL's territorial requirements. These tools help manage the risks associated with international transfers, ensuring data remains within compliant boundaries.

The capabilities include:

- **Visibility into data transfers**: Netskope's DLP engine, supported by advanced analytics, provides complete visibility into personal data flows, ensuring that cross-border transfers are monitored and controlled.
- **Risk assessment for cloud providers**: The Netskope CCI scores SaaS applications and cloud services based on their security posture, certifications, and compliance with legal and privacy regulations, helping organizations assess the risk of using third-party services.

- **Enforcement of data residency**: Netskope supports data localization policies, with both data and management planes available from our Saudi Arabian data centers located in Jeddah and Riyadh, ensuring that personal data remains within Saudi Arabia's geographic boundaries, in line with the PDPL's requirements.

By simplifying the management of international data transfers and ensuring compliance with data residency laws, Netskope enables organizations to maintain operational flexibility while adhering to the PDPL's strict cross-border data transfer rules.

Advanced Protection for Sensitive and High-Risk Personal Data

The PDPL mandates strict protections for sensitive personal data, including health, genetic, and biometric information. Netskope's DLP and encryption capabilities ensure that sensitive data is protected both in transit and at rest, significantly reducing the risk of unauthorized access or misuse.

These protections are essential for organizations handling highly regulated data, ensuring compliance with the PDPL's stringent security requirements and offering the following benefits:

- **Find sensitive data anywhere**: Netskope automates data security and governance controls in the cloud and on-premises, for structured, semi-structured, and unstructured data. Providing visibility and control for data infrastructure, data attributes, data users, and data usage.
- **Automated sensitive data protection**: The Netskope One DLP engine leverages machine learning and advanced analytics to simplify data classification and accelerate policy implementation to protect sensitive personal data, ensuring it remains secure at all times.
- **Real-time access control**: Netskope One Zero Trust Engine enforces real-time, context-driven access control based on zero trust principles by continuously monitoring and adjusting access levels to ensure only authorized personnel can access sensitive data. This provides organizations with granular visibility, adaptive access control, and streamlined data protection, reducing risks and operational costs.
- **End-to-end encryption**: With Netskope One Private Access, organizations can ensure the confidentiality and integrity of sensitive data by encrypting it both in transit and at rest, significantly reducing the risk of unauthorized access even in the event of a security breach.
- **Reliable detection and classification data**: The Netskope One DLP engine leverages machine learning for identifying and protecting personal data according to organizational and regulatory standards with over 3,000 predefined data identifiers and personal identifiers. Enabling organizations to detect well-known data patterns such as personal IDs and credit cards, to sensitive personal data, including health, genetic, and biometric information.

Netskope's advanced data protection measures allow organizations to safeguard sensitive personal data, mitigate risks, and comply with the PDPL's stringent security controls.

Comprehensive Compliance Management and Record-Keeping

Under the PDPL, maintaining accurate records of data processing activities is essential, particularly for high-risk processes that require Data Protection Impact Assessments (DPIAs). Netskope's solutions, including export capabilities and automated compliance reporting, enable organizations to maintain comprehensive records of their data processing activities.

These tools help demonstrate compliance during audits and ensure that organizations can meet their legal obligations and provide:

- **Comprehensive record-keeping**: Netskope's DLP engine tracks data processing activities across web, cloud, and endpoint environments, ensuring full visibility into personal data handling and compliance with PDPL record-keeping requirements.

- **Automatic data classification and tagging**: Netskope One DSPM automatic classification and tagging streamlines compliance and allows increased focus on business-critical objectives. The simple no-code policy engine enables security and compliance teams to set up rules and workflows for various aspects, such as shadow data store discovery, misconfiguration, data classification, data access violations, and data-in-use monitoring.
- **Automated compliance reporting**: Detailed reports and audit trails streamline the process of demonstrating compliance with the PDPL, making it easier to respond to data subject access requests (DSARs) and regulatory inquiries.
- **Netskope Cloud Exchange integration**: The Netskope One platform's export capabilities ensure that records of processing activities are accurate, up to date, and easily accessible during audits or compliance reviews.

Netskope's record-keeping and accountability features ensure that organizations can maintain transparency, meet regulatory demands, and effectively manage the risks associated with non-compliance.

Conclusion

Netskope's comprehensive security solutions address the core data protection challenges under the SDAIA PDPL, from real-time breach detection and secure cross-border data management to sensitive data protection and detailed record-keeping. With the world's largest, high-performance private security cloud powered by data centers in 75+ regions, Netskope provides robust, scalable protection and regulatory compliance. Available from our data centers in Jeddah and Riyadh, Netskope ensures that personal data remains within Saudi Arabia's boundaries, enabling organizations to enhance their data protection posture while meeting PDPL requirements with confidence.