

SECLORE™

Complying with the Personal Data Protection Law (PDPL) Using Seclore's Data-Centric Security Platform



Executive Summary

Saudi Arabia's Personal Data Protection Law emphasizes safeguarding personal data. Compliance with this law also requires that organizations put stringent data collection, processing, storage, and destruction measures in place. A data-centric security approach helps ensure data protection is built into every process involving personal data. Seclore provides advanced data protection solutions that include encryption, access controls, and enterprise digital rights management (EDRM). These solutions help organizations comply with the law in a way that also improves their cybersecurity, an outcome that we refer to as "compliance-driven protection."



Introduction

The Personal Data Protection Law (PDPL) is the first comprehensive data protection law in Saudi Arabia. The Saudi Data and Artificial Intelligence Authority (SDAIA) is expected to begin enforcing the PDPL on September 14, 2024, after the current compliance grace period ends. SDAIA emphasized that it expects entities to take measures to achieve compliance with the PDPL before the September deadline.

The Personal Data Protection Law mandates rigorous controls over personal data to protect the privacy of individuals. This white paper outlines key provisions of the PDPL, the role of data-centric security, and how Seclore can help organizations achieve compliance.

Key Provisions of the Personal Data Protection Law (PDPL)

Scope of the PDPL

The PDPL has a vast scope and applies to all entities operating in Saudi Arabia, as well as entities outside of Saudi Arabia that process the personal data of individuals in Saudi Arabia (without a requirement to target or monitor the individuals). All in-scope entities must complete a compliance program before **September 14, 2024**.



Personal Data

Any data, regardless of its source or form, that may lead to identifying an individual specifically or that may directly or indirectly make it possible to identify an individual, including name, personal identification number, addresses, contact numbers, license numbers, records, personal assets, bank and credit card numbers, photos and videos of an individual, and any other data of personal nature.



Processing

Any operation carried out on Personal Data by any means, whether manual or automated, including collecting, recording, saving, indexing, organizing, formatting, storing, modifying, updating, consolidating, retrieving, using, disclosing, transmitting, publishing, sharing, linking, blocking, erasing and destroying data.



Sensitive Data

Personal Data revealing racial or ethnic origin or religious, intellectual, or political belief; data relating to security criminal convictions and offenses; biometric or Genetic Data to identify the person; Health Data, and data that indicates that one or both of the individual's parents are unknown.



Rights of Data Subjects

- Right to be informed about data collection and processing.
- Right to access, correct, or request the destruction of personal data.
- Consent requirements for data processing and withdrawal of consent.



Obligations of Controllers and Processors

- Controllers must ensure data is collected lawfully and processed only for specified purposes.
- Adequate protection measures, including data encryption and access controls, must be in place.
- Mandatory breach notification to the competent authority and affected data subjects.

Data-Centric Security

In today's digital landscape, data is as valuable as currency, and those who steal it are the modern equivalent of early 20th-century bank robbers. Traditional data security solutions, such as [data loss prevention \(DLP\)](#), primarily rely on perimeter-based defenses. These tools, which include network, endpoint, and cloud security, focus on building a protective barrier around your data to prevent unauthorized access and exfiltration.

However, data-centric security takes a more comprehensive approach by protecting data at the core, regardless of the user, device, application, or cloud environment involved. Unlike perimeter-based solutions, data-centric security ensures continuous protection and provides real-time insights into data usage, even as information moves beyond the organizational boundary to external partners.

The stakes are high—recent statistics show that the [average cost of a data breach](#) in the Middle East has reached 29.9 million SAR. Securing your enterprise against data exfiltration is essential, but the challenge lies in the fact that most traditional security solutions are designed to prevent unauthorized entry into systems. Once attackers bypass these perimeter defenses often gain nearly unrestricted access to sensitive, business-critical information.

The emergence of the Personal Data Protection Law in Saudi Arabia mandates a transformative approach to handling personal data. To comply with the law and protect sensitive information, organizations should employ a comprehensive data protection solution that includes Data Loss Prevention (DLP), [Data Classification](#), [Enterprise Digital Rights Management \(EDRM\)](#), and Security Information and Event Management (SIEM) systems.



Data Loss Prevention (DLP)

Data Loss Prevention (DLP) solutions discover sensitive data and block it from leaving your organization. DLP can control the flow of information and prevent sensitive data from leaving the perimeter. However, it doesn't provide end-to-end security and can reduce productivity. Once your sensitive data is shared outside your organization with contractors, vendors, and partners – you've lost control of your data. Integrating DLP with data-centric security allows for more granular control, ensuring that data remains encrypted and inaccessible to unauthorized users even if it slips through the DLP filters.



Data Classification

Data classification is essential for safeguarding sensitive information, ensuring regulatory compliance, and optimizing resource allocation and incident response. Businesses can effectively protect their valuable information assets by categorizing data based on sensitivity and importance. Data classification helps organizations identify and safeguard sensitive data while preventing unauthorized access and theft. Adding data-centric security to data classification enables organizations to apply appropriate security levels to different classification labels to ensure regulatory compliance and prevent unauthorized access to sensitive data.



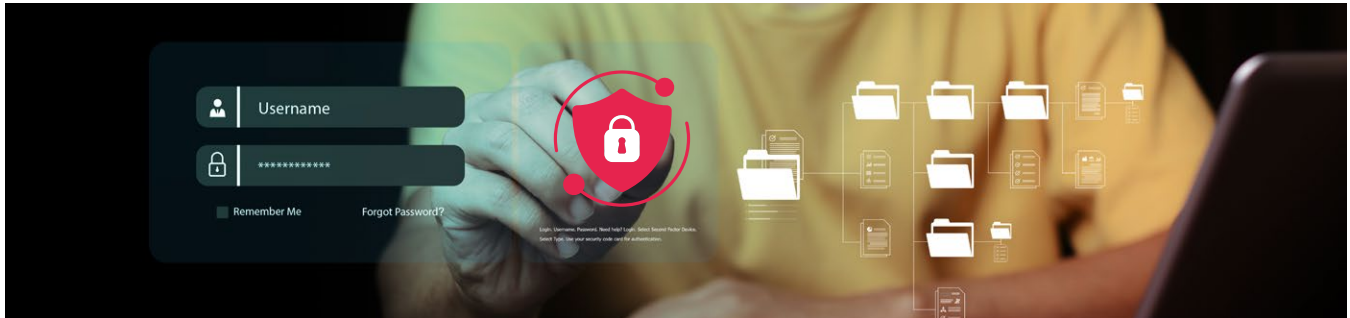
Enterprise Digital Rights Management (EDRM)

Enterprise Digital Rights Management (EDRM) refers to the systems and processes that govern the enterprise's access and usage of sensitive digital assets. Sometimes called information rights management (IRM), it's a distinct form of digital rights management (DRM) designed to fulfill the needs of businesses. Data-centric security adds a layer of protection, ensuring data security beyond the controls of EDRM.



Security Information and Event Management (SIEM)

Security Information and Event Management (SIEM) solutions help rapidly detect, invest, and respond to security incidents. SIEM environments act as real-time event aggregators and vigilant watchdogs for unauthorized IT and OT activity. They usually collect and analyze data from multiple sources, including network logs, user activity, business applications, and APIs. Data-centric security enables organizations to track user activity wherever the assets are. Data-centric visibility lets security and compliance teams proactively protect their organization's most sensitive data and helps Security Operations Center (SOC) teams get the most out of their SIEM investments with more granular visibility.



Seclore's Data-Centric Security Platform

Data-centric security solutions intelligently apply protection as near to sensitive data as possible. These solutions provide continuous protection and visibility that emphasize protecting sensitive information at the file level. This approach can be likened to a safe deposit box with a camera pointed at it for each bill held in a bank's vault. With [Seclore's data-centric security approach](#), data is protected no matter where it goes because Seclore's safe deposit box goes wherever the data does — so digital assets remain secure across any user device, network, app, or cloud environment.

Know

Seclore provides detailed audit logs and reports on data access and usage so organizations can demonstrate compliance with their legal and regulatory requirements. These logs are crucial for responding to a data subject's request for information and regulatory audits.

Protect

Seclore uses robust encryption protocols for protected files and emails to ensure that data remains secure at rest, in transit, and use. This aligns with Article 19 of the law, which mandates technical measures to protect personal data.

Control

Seclore supports granular access controls that allow organizations to specify who can access specific files, what they can do with the data contained in those files, and for how long. This helps prevent unauthorized users from accessing or sharing data, which is crucial for complying with Article 10 (which states that only authorized personnel can access personal data).

- Dynamic watermarking adds visible watermarks to documents to discourage unauthorized distribution and ensure traceability.
- Dynamic permissions let organizations modify access and usage controls in near real-time, allowing them to react quickly to new information or changed circumstances.

How Seclore Helps Organizations Comply with the PDPL

Data Visibility

Understanding where your data is stored, who has access to it, and how it is being used is the first step toward ensuring compliance and protecting personal information. The PDPL mandates that organizations must be transparent and meticulous in managing personal data and even grants individuals rights such as the right to access, correct, and delete their data.

To meet these requirements, robust mechanisms must be in place to track and manage consent and preserve detailed records of data processing activities. Seclore provides granular activity information, empowering organizations to efficiently respond to data subject requests, maintain comprehensive records, and manage consent. With complete visibility, you can meet PDPL's stringent requirements and safeguard the trust and privacy of your customers.

Article	Requirement	How Seclore Can Help
Article 4	Data Subject Rights (Access, Correct, Delete)	Seclore helps organizations protect, manage access, and track protected digital assets containing regulated personal information. With Seclore, organizations can give data subjects easier access to their personal information and verify access or deletion status with their auditors. Seclore provides detailed audit trails and reports, including user, machine name, IP address, and timestamps for protected digital assets, and allows for remote access revocation.
Article 5	Consent Management	Seclore prevents unauthorized access by persistently protecting digital assets on any machine, network, or cloud environment, ensuring that only authorized users can access protected digital assets. Seclore can also integrate directly with existing data discovery and classification tools to apply protection and usage controls based on classification or sensitivity labels.
Article 20	Breach Notification	Seclore gives organizations detailed usage and activity information for protected digital assets. This incredibly granular telemetry can be synchronized with an SIEM system and combined with other information, such as network activity, to alert organizations to suspicious or unusual activity. Seclore's Risk Insights dashboard also allows organizations to spot unusual activity related to protected digital assets, which could indicate a breach, insider threat, or compromised credentials.
Article 31	Record Keeping	Seclore tracks all user activity related to protected digital assets and provides comprehensive downloadable audit trails and reports that include user details, machine names, IP addresses, and timestamps. This information can also be synchronized as a BI tool for long-term storage and discoverability.

Data Protection

Protecting sensitive data means implementing robust security measures to ensure that personal data is secure throughout its lifecycle — whether collected, processed, stored, or transferred.

PDPL requires that organizations take proactive steps to safeguard data integrity, mainly when dealing with sensitive information such as health and credit information. This involves employing encryption, access controls, and other security measures to prevent unauthorized access and breaches. Seclore’s comprehensive data-centric security solution enables organizations to meet these requirements by automatically encrypting data collected or processed and applying stringent access controls to that data. Prioritizing the protection of sensitive data can help you comply with PDPL and build a stronger defense against potential data breaches and leakage.

Article	Requirement	How Seclore Can Help
Article 6	Processing without Consent	Seclore limits authorized users' access to protected digital assets, preventing unauthorized users from processing sensitive data without consent.
Article 10	Data Collection and Processing	Seclore can protect personal data when it’s collected or processed for lawful purposes. It enables encryption and audit trails to better protect the integrity of that data. Protection can be automated through email, collaboration tools, or a data protection portal.
Article 19	Data Protection Measures	Seclore natively supports multi-layered encryption and custom encryption protocols. Seclore uses two secure and compliant encryption algorithms, AES 256 and RSA 2048. Seclore EDRM also protects any copies of protected digital assets regardless of how they are created, whether by email, USB, shared folder, or any other method — which means that sensitive digital assets are always protected, even if they are shared with external parties or exfiltrated as part of a breach.
Article 23	Health Data Processing	Seclore offers additional controls for processing health data, ensuring compliance with stringent privacy requirements.
Article 24	Credit Data Processing	Seclore ensures that credit data processing meets the privacy standards outlined in the law, including consent management and data protection.

Data Control

The ability to control who can access, share, or delete personal data is fundamental to maintaining data security and privacy. PDPL mandates strict guidelines for data sharing, transfer, and destruction, requiring organizations to have precise control mechanisms.

Using Seclore, organizations can enforce granular access controls, securely manage data transfers, and ensure data is deleted per legal standards. These capabilities are essential for preventing unauthorized data disclosures and ensuring that data is handled according to organizational policies and legal requirements. By exercising tight control over protected personal information, organizations can ensure compliance with PDPL and mitigate the risks associated with improper data handling, thereby protecting your organization from potential legal and financial repercussions.

Article	Requirement	How Seclore Can Help
Article 15	Data Disclosure	Seclore provides access controls to prevent unauthorized data disclosure by restricting access and ensuring that data sharing and disclosure policies comply with legal requirements. Seclore can also further restrict access, apply dynamic watermarks, and limit printing, copying, and saving local copies to help prevent unauthorized data disclosures.
Article 18	Data Destruction	With Seclore, Information owners can permanently or temporarily revoke access to protected digital assets shared with anyone, including internal users, external agencies, partners, or contractors, effectively 'destroying' that data. Seclore also provides audit trails that enable organizations to prove who had access to sensitive data, for how long, and whether that information has been effectively destroyed.
Article 21	Responding to Data Subject Requests	Seclore provides the tools to efficiently manage and respond to data subject requests within the specified timeframe.
Article 27	Scientific and Statistical Processing	Seclore supports the secure processing of personal data for scientific and research purposes, ensuring integrity and data protection.
Article 29	Data Transfer	Seclore provides tools for secure data transfer, ensuring that data shared outside the Kingdom meets protection standards.
Article 35	Penalties for Data Breaches	Seclore's robust security measures reduce the risk of breaches, helping organizations avoid penalties for non-compliance.
Article 37	Violation Monitoring	Seclore supports compliance monitoring and enforcement, helping organizations adhere to legal standards.

Conclusion

Seclore's data-centric security platform has been proven to:



Help organizations protect their confidential information.



Eliminate data leakage and theft, especially for outsourced business operations.



Improve compliance and reporting capabilities with the relevant guidelines and auditors.

Compliance with the Personal Data Protection Law requires a robust data protection framework that includes encryption, access controls, and detailed monitoring. Seclore's data-centric security platform provides the tools to protect personal data, ensure compliance, and prevent data breaches. By integrating Seclore's solutions, organizations can enhance their data protection measures and confidently navigate this regulatory landscape.





About Seclore

Our mission is to safeguard sensitive information worldwide, regardless of its location. Seclore offers persistent protection and visibility for digital assets to help organizations remain secure and compliant. Our data-centric security approach ensures that only authorized individuals can access protected digital assets. With Seclore, organizations can specify who can access their data, what actions are permitted, and how long that access lasts. Join industry leaders like American Express in choosing Seclore for superior digital asset protection without sacrificing seamless collaboration and sharing.

Visit seclore.com for more information.

5201 Great America Parkway
Suite 440
Santa Clara, CA 95054