Navigating Sri Lanka's PDPA with Logical Data Management

Sri Lanka, with a population of approximately 22 million, is strategically positioned to leverage its digital economy for economic growth and development, as evidenced by recent statistics and government initiatives. As of January 2025, the country boasts 12.4 million internet users, representing a 53.6% penetration rate, and 8.2 million social media users, indicating a robust digital presence (Digital 2025: Sri Lanka — DataReportal). This growth is supported by the National Digital Economy Strategy 2030, approved on March 25, 2024, which aims to transform Sri Lanka into a digital powerhouse by enhancing economic competitiveness, creating employment opportunities, and driving sustainable development through digital transformation (The National Digital Economy Strategy - 2030 for Sri Lanka | Ministry of Digital Economy). This strategy underscores the country's commitment to leveraging technology for economic recovery and resilience, particularly in the context of recent economic challenges.

Sri Lanka's Personal Data Protection Act (PDPA), No. 9 of 2022, certified on March 19, 2022, establishes a robust framework for safeguarding personal data in the digital economy. Originally intended to be effective in phases—18 to 36 months for most provisions and 24 to 48 months for Part IV—the implementation of Sri Lanka's Personal Data Protection Act (PDPA) No. 9 of 2022 has experienced delays. Specifically, Parts I, II, III, and VII, which were scheduled to come into effect on March 18, 2025, have had their enforcement date repealed as per Extraordinary Gazette No. 2427/34 issued on March 14, 2025. However, organizations need to be prepared for compliance now - as enforcement may occur in the very near future. Non-compliance can incur penalties up to LKR 10 million per violation (Section 38).

The PDPA defines personal data as information identifying an individual, including general data (e.g., name, ID number) and special categories (e.g., biometric, health, genetic data). Processing special categories requires explicit consent or legal grounds per Schedules I and II. Organizations must appoint a Data Protection Officer for large-scale or sensitive data processing and conduct impact assessments (Section 24).

Key Roles Specified in the PDPA

- **Data Subject:** Individuals associated with personal data, defined as any information relating to an identified or identifiable individual, whether directly or indirectly, through electronic or non-electronic means (Section 49).
- **Personal Data Controller:** Any person, public body, or organization, acting individually or jointly, that determines the purposes and means of processing personal data (Section 21).

SOLUTION
PDPA Compliance

INDUSTRY
Applicable to all companies doing business with Sri Lankan entities

WEBSITE
www.denodo.com

PRODUCT OVERVIEW
Denodo is a leader in data management. The award-winning Denodo Platform is the leading logical data management platform for transforming data to trustworthy insights and outcomes for all data-related initiatives across the enterprise, including AI and self-service. Denodo's customers in all industries all over the world have delivered trusted AI-ready and business-ready data in a third of the time and with 10x better performance than with lakehouses and other mainstream data platforms alone.

- **Personal Data Processor:** Any person, public body, or organization processing personal data on behalf of a controller, acting under a formal agreement. Processors cannot independently determine the purposes or means of processing (Section 22).

- **Data Protection Officer:** An officer appointed by the controller or processor to ensure compliance with the PDPA, required for large-scale or sensitive data processing. The DPO may be internal or external to the organization (Section 20).

Key Principles of the PDPA

To define the scope of compliance, the PDPA outlines several key principles that govern the processing of personal data:

- **Lawfulness, Fairness, and Transparency:** Data must be processed lawfully, fairly, and transparently, with clear communication to data subjects (Section 7).

- **Purpose Limitation:** Data should be collected for specific, legitimate purposes and not processed in ways incompatible with those purposes (Section 7).

- **Data Minimization:** Only data that is relevant and necessary for the specified purposes should be processed (Section 7).

- **Accuracy:** Personal data must be accurate and kept up-to-date, with measures to correct inaccuracies (Section 8).

- **Integrity and Confidentiality:** Data must be processed securely, protecting against unauthorized access, loss, destruction, or damage (Section 10).

The PDPA grants data subjects rights to be informed about data collection, access their data, correct inaccuracies, request erasure, restrict processing, and object to processing, including automated decision-making (Sections 13-19). They can withdraw consent, appeal to the Data Protection Authority, and seek remedies for violations without discrimination. The PDPA restricts cross-border data transfers, requiring adequacy decisions or safeguards for non-public entities, while public authorities must process data locally unless approved (Section 26). This poses challenges for multinational organizations with centralized data systems. Many organizations, especially small and medium-sized enterprises, face difficulties upgrading data protection systems, drafting privacy policies, and enhancing cybersecurity. Failure to comply risks significant penalties and reputational damage.

Sri Lanka's PDPA and Data Management Challenges

- **Legal Basis:** Processing requires consent or lawful grounds (e.g., public interest) per Schedules I and II.

- **Consent and Transparency:** Consent must be freely given and informed, with opt-out options (Schedule III, Sections 11, 13).

- **Cross-Border Data Flows:** Public authorities process data locally unless approved; non-public entities need adequacy decisions or safeguards (Section 26).

- **Security and Breach Notification:** Encryption and access controls are mandatory, with breach reporting to the Authority (Sections 10, 23).

- **Data Subject Rights:** Individuals can access, rectify, erase, or object to processing, with appeals to the Authority (Sections 13-19).

- **Controller and Processor Accountability:** Processors must follow controller instructions via formal agreements (Sections 21, 22).

Organizations struggle with fragmented data, integration costs, and security risks across hybrid environments, complicating PDPA compliance.

Limitations of Centralized Architectures for PDPA Compliance

Many organizations rely on centralized architectures like data lakehouses for their data strategies, but these are not specifically designed for PDPA compliance. While lakehouses offer scalability for analytics, they present key challenges in enabling effective data governance, regulatory tracking, and real-time access to sensitive data:

- **Data Processing Delays:** Data lakehouses require data to be onboarded and transformed before use, causing delays that hinder real-time access needed for PDPA-compliant governance, auditing, and breach notifications (Sections 11, 23).
- **Hybrid and Multi-Cloud Complexities:** PDPA mandates controlled data sovereignty, particularly for public authorities processing data locally (Section 26). Managing compliance across geographically distributed hybrid or multi-cloud systems is inefficient and costly with lakehouses alone.
- **Regulatory Burdens:** PDPA requires tracking data lineage, storage, transfers, and access for impact assessments and accountability (Sections 12, 24). Lakehouses lack built-in compliance controls for regulatory audits and reporting.
- **Data Silos and Distributed Sources:** Data often resides outside lakehouses, such as during mergers or in multi-cloud setups. Replicating this data via extract, transform, and load (ETL) processes increases complexity and costs, conflicting with PDPA's data minimization principle (Section 7).

Logical Data Management with the Denodo Platform for Seamless PDPA Compliance

The Denodo Platform, the leading logical data management platform, unifies disparate data into a single access layer, enabling efficient data discovery and consumption. It embeds governance and security controls, ensuring PDPA compliance without sacrificing agility.

A UNIFIED SEMANTIC LAYER

The Denodo Platform connects to diverse data sources in real time, creating a unified semantic layer that delivers business-friendly data. Governance policies are enforced automatically, streamlining PDPA reporting (Section 11).

CENTRALIZED CONTROL

Stakeholders manage all data sources from one point, enforcing PDPA-compliant privacy and security policies across hybrid environments, simplifying compliance (Section 12).

REAL-TIME TRACKING

Real-time data access supports instant alerting and usage reports, enabling rapid response to PDPA breaches (Section 23).

CONSOLIDATED REGULATORY REPORTING

Unified data access enables comprehensive reporting, including lineage tracking, supporting PDPA transparency and impact assessments (Sections 11, 24).

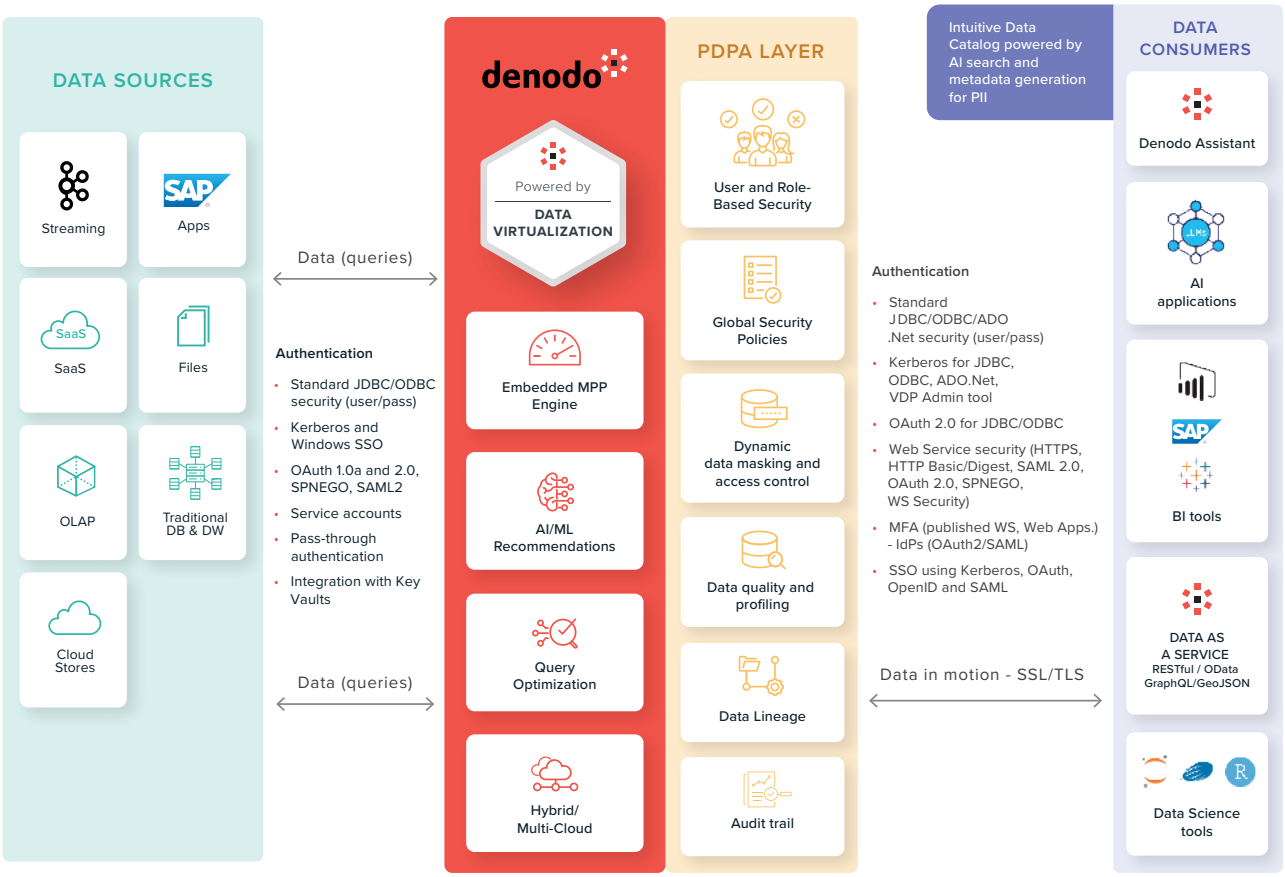
ROLE- AND ATTRIBUTE-BASED ACCESS CONTROLS

Policies based on roles and attributes (e.g., location) ensure precise control, aligning with PDPA security requirements (Section 10).

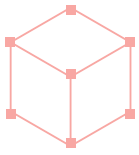
GLOBAL POLICIES

Semantic security policies (e.g., masking, encryption) facilitate compliance with PDPA's measures for special categories and cross-border transfers (Sections 10, 26).

How the Denodo Platform can Help Meet PDPA Requirements



ROLE	DENODO PLATFORM BENEFITS
DATA SUBJECT	■ Assurance that personal data is protected with minimal, purpose-specific usage. ■ No unnecessary replication, aligning with data minimization (Section 7).
PERSONAL DATA CONTROLLER/ DATA PROCESSOR	■ Support for RBAC, ABAC, and global security policies. ■ Real-time monitoring of data access (Section 12). ■ Data profiling to detect inaccuracies (Section 8). ■ Encryption at rest and in transit (Section 10). ■ Denodo Assistant recommends datasets and describes sensitive data.
DATA PROTECTION OFFICER	■ A powerful data catalog that provides a simple search mechanism for an intuitive discovery process ■ The ability to query data using natural language ■ An audit trail with full lineage support for data processed both on- and off-premises (section 24) ■ Metadata search and recommendations for special categories (Schedule II).



CASE STUDIES

Toyota Astra Motor (TAM), the leading automotive distributor in Indonesia, manages sensitive customer and vehicle data across its sales and after-sales networks. As data privacy expectations continue to grow, TAM sought to simplify its complex data landscape and strengthen governance across its operations.

TAM implemented the Denodo Platform to seamlessly integrate multiple source systems and create a centralized access layer. This modern data architecture improved data integrity and trust while enabling real-time visibility into the business.

In addition to enhancing operational resilience and self-service analytics, the Denodo solution enabled user-activity auditing and real-time monitoring – capabilities that support many of the core requirements of Sri Lanka's PDPA.

By embedding these controls within its data delivery layer, TAM is better positioned to manage sensitive data responsibly and strengthen readiness for current and future data protection regulations, including PDP.

DNB

DNB, Norway's largest financial services group, needed to support strict GDPR requirements while modernizing access to sensitive customer data across AWS, on-premises data warehouses, Kafka, Cloudera, Neo4j, and APIs. A key challenge was enabling over 150 analysts and data scientists to build models – such as those handling churn prediction, fraud detection, and personalized pricing – while keeping customer PII fully compliant with GDPR.

Previously, data scientists spent significant time preparing and integrating data from disparate systems. At the same time, DNB had to ensure that all use of sensitive personal data adhered to GDPR principles, including purpose limitation, data minimization, and access control.

> *"The Denodo Platform eased data integration and data sharing and has provided a self-service data platform that follows data mesh principles."*
>
> **Olav Lognvik,** Lead Architect at DNB

By deploying the Denodo Platform as a logical data marketplace, DNB provided governed, real-time access to distributed data. Denodo enabled role- and attribute-based access controls, data masking, and audit-ready tracking of data usage across users and tools.

The Denodo Platform's semantic layer and data catalog further accelerated discovery and self-service, with embedded governance.

Denodo helped DNB meet GDPR requirements while reducing time-to-insight, improving security, and scaling governed access to sensitive data across operational and analytical domains.

GetSmarter, a leading provider of accredited online student courses, experienced rapid growth that led to a fragmented data ecosystem spanning microservices, SaaS platforms, cloud infrastructure, and legacy systems. As the company scaled across Europe and Africa, it faced increasing regulatory pressure to comply with data privacy laws such as the European Union's GDPR and South Africa's Protection of Personal Information Act (PoPIA).

To simplify governance, strengthen security, and meet its data protection obligations, GetSmarter implemented the Denodo Platform as a unified data access layer. This enabled secure, real-time access to data across all systems – without physical replication – while enforcing centralized data protection policies and policy-based controls to manage sensitive data. It also accelerated delivery of governed data for analytics and reporting.

With the Denodo Platform, GetSmarter was able to:

- Apply granular role- and attribute-based access controls
- Enable data masking and anonymization for sensitive PII
- Create centralized audit trails and data lineage for compliance reporting
- Establish a single semantic model for consistent, trusted data views

> *"The Denodo Platform on the AWS Marketplace lets us impose granular access controls for both users and systems, so our compliance with GDPR and other data protection requirements is even stronger."*
>
> **Schoeman Loubser,** Former Information Architect, Data Infrastructure and Analytics at GetSmarter

The same capabilities that helped GetSmarter meet GDPR and PoPIA obligations – such as consent-driven access, purpose limitation, and secure processing – are fully aligned with Sri Lanka's PDPA, making Denodo a strong fit for organizations navigating similar regulatory requirements.

asurion

Asurion, a global leader in technology support services, needed to modernize its infrastructure to support cloud analytics while maintaining strict compliance with international data protection regulations. The company faced limitations in migrating personally identifiable information (PII) to the cloud due to regulatory restrictions and needed a solution that could enforce centralized security and governance across hybrid environments.

By implementing the Denodo Platform, Asurion established a virtual data access layer that unified cloud and on-premises data sources under a single point of control. This architecture enabled policy-based security, including row- and column-level access control, encryption, and data masking, all essential for managing sensitive data.

> *"The Denodo Platform was one of the easiest and most successful rollouts of critical enterprise software I have seen, and it was immediately successful in handling our initial security use case."*
>
> **Enterprise Architect**, Asurion

Denodo helped Asurion fulfill regional compliance obligations by enabling:

- Auditable access trails across all user interactions
- Role-based data permissions
- Rapid onboarding of compliant data sources
- Centralized enforcement of data minimization and purpose-based access

With the Denodo Platform, Asurion simplified enterprise-wide security governance and only enabled access to sensitive data when explicitly authorized. These capabilities directly support key principles under Sri Lanka's PDP Law, including consent-based processing, auditability, real-time access control, and data protection without unnecessary duplication.