Navigating Thailand's PDPA with Logical Data Management

Thailand's Personal Data Protection Act (PDPA) became law on May 28, 2019, and came into full force on June 1, 2022, following multiple extensions. The law aligns closely with the EU's General Data Protection Regulation (GDPR) but includes unique provisions tailored to Thailand's regulatory environment. It applies to organizations collecting, using, or disclosing personal data in Thailand or of Thai residents, regardless of their physical location.

The PDPA defines personal data as any information that can identify an individual, either directly or indirectly. It distinguishes between general and sensitive personal data, with the latter—including race, health data, biometric data, and criminal records—requiring stricter security measures and explicit consent for processing. The law mandates organizations to uphold transparency, data minimization, and purpose limitation while ensuring data subjects' rights are protected.

The Personal Data Protection Committee (PDPC) oversees PDPA enforcement and issues subordinate regulations to clarify compliance requirements. The PDPA requires businesses to appoint a Data Protection Officer (DPO) if they engage in large-scale data processing or process sensitive personal data regularly. Organizations failing to comply with PDPA requirements may face administrative fines of up to THB 5 million, along with criminal penalties in severe cases.

Thailand's PDPA and Data Management Challenges

- **Legal Basis for Data Processing:** Organizations must obtain explicit consent to collect, use, or disclose personal data unless exemptions apply (e.g., contract fulfillment, legal obligations, or legitimate interests). Sensitive personal data requires stricter compliance and explicit consent.
- **Consent and Transparency:** Consent must be clear, explicit, and separate from other agreements. Data subjects must be informed of how their data is collected, processed, and stored, with the right to withdraw consent at any time.
- **Data Residency and Cross-Border Transfers:** Personal data transfers outside Thailand require either regulatory approval or safeguards like Binding Corporate Rules (BCRs) to ensure adequate protection.
- **Security and Breach Notification:** Organizations must implement robust security measures, including encryption, access controls, and periodic reviews. Data breaches must be reported to the PDPC within 72 hours if they pose high risks to data subjects.

SOLUTION
PDPA Compliance

INDUSTRY
Applicable to all companies doing business with Thai 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.

- **Data Subject Rights:** Individuals can access, correct, delete, or transfer their data. They can also object to processing and automated decision-making.
- **Processor Accountability:** Data Controllers must ensure that Data Processors comply with PDPA regulations through formal agreements.

Many businesses struggle with fragmented data sources, high integration costs, and security risks across hybrid environments, making compliance a challenge.

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, serving as the single place where all data consumers in the business can discover and consume the data they need.

The Denodo Platform enables organizations to define and enforce comprehensive access controls, reporting, auditing, and other actionable risk and compliance management activities directly from this same layer, leveraging data in the same structure and format that the business has defined.

By embedding data governance and compliance in the same layer that delivers data to the business, companies can achieve compliance and manage risks across all data sources and silos, without sacrificing agility and competitiveness.

A Unified Semantic Layer

The Denodo Platform connects to disparate data sources in real time to seamlessly establish a unified semantic layer that provides business users with data in the language of the business, at the speed that the business requires. In the view enabled by this unified semantic layer, all data governance and compliance policies are automatically enforced, regardless of where the data is stored.

Centralized Control

With the ability to access and manage all data sources from a single point of control, stakeholders can enforce data privacy, data governance, and security policies across all data sources without the time-consuming, error-prone work of implementing policies in each individual data source.

Real-Time Tracking

With real-time access to data, the Denodo Platform supports real-time alerting and continuously updated usage reports. Administrators can set thresholds to trigger automatic actions, or immediately respond to PDPA violations or potential breaches. The Denodo Platform gives organizations the upper hand in all governance, risk, and compliance activities.

Consolidated Regulatory Reporting

By unifying access to disparate data sources, the Denodo Platform enables consolidated reporting for all stakeholders and external regulatory bodies, including financial reporting; environmental, social and governance (ESG) reporting; sustainability reporting; and data privacy compliance reporting. Such reports can include data lineage and usage tracking, all the way back to the original source systems, for additional compliance support.

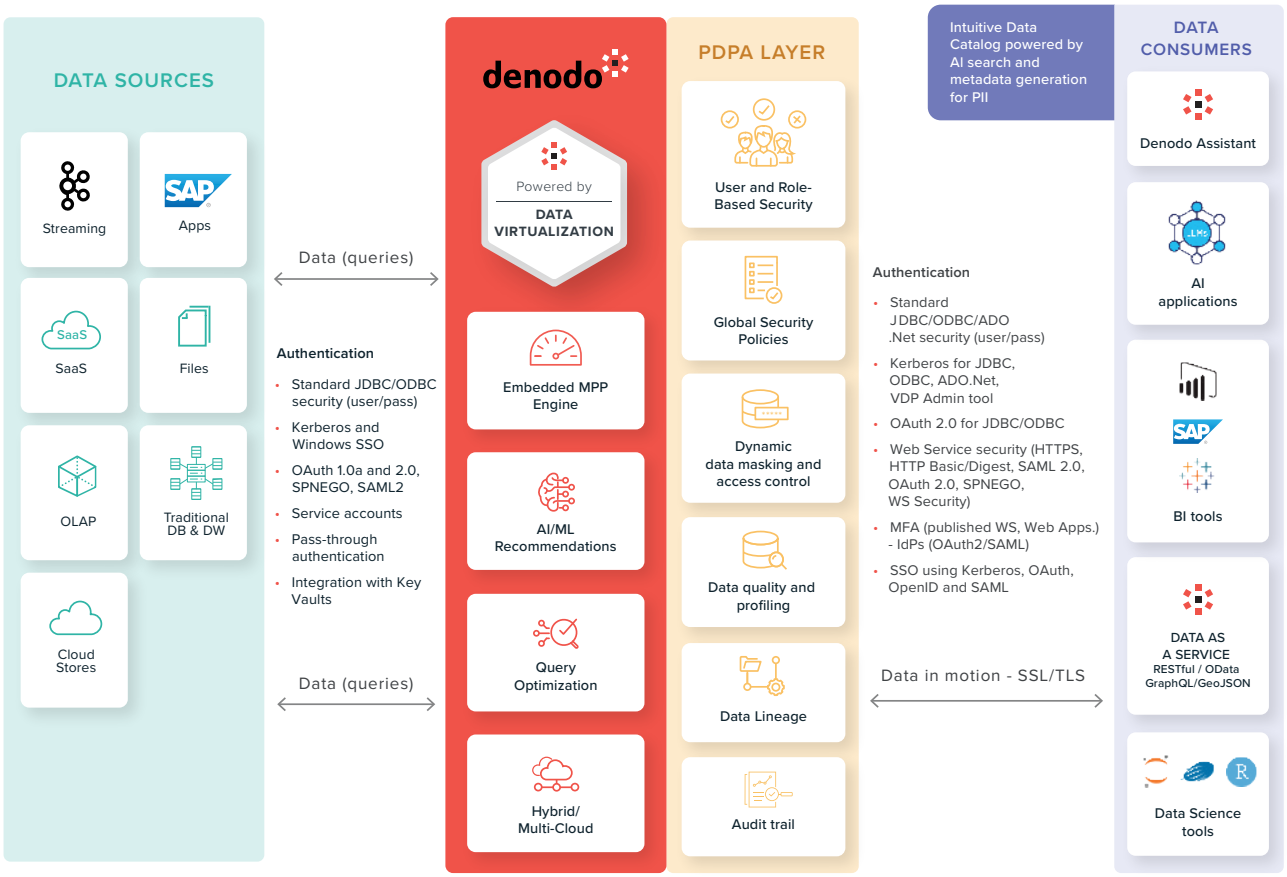
Role- and Attribute-Based Access Controls

Access policies can be defined based on user roles as well as user attributes, such as organization, physical location, project codes, and other parameters. For example, employees working from home or on business travel may not have the same level of access that they have when they are in the office or on a secure network.

Global Policies

The Denodo Platform enables the definition of global policies based on view or column attributes within the semantic layer, allowing for precise control over data access. These include semantic security policies for masking, encryption, and data restrictions, facilitating compliance with security classifications and business requirements. These capabilities greatly assist in meeting the stringent data security measures required by the PDPA.

How the Denodo Platform can Help Meet PDPA Requirements



ROLE	DENODO PLATFORM BENEFITS
DATA SUBJECT	■ Peace of mind that personal data is protected ■ Data does not need to be replicated - It is used and collected only for a specific purpose, and usage is minimized
PERSONAL DATA CONTROLLER/ DATA PROCESSOR	■ Comprehensive support for RBAC, ABAC, and global security policies ■ The ability to monitor who is accessing personal data ■ The ability to implement data rules for out-of-compliance situations. ■ A data profiling tool to help detect inaccuracies ■ Data can be secured and encrypted at rest and in transit ■ The Denodo Assistant, an AI-powered assistant, can recommend relevant datasets and even create AI-generated descriptions of views and columns – including those which contain sensitive information
DATA PROTECTION OFFICER	■ A powerful, e-commerce-style Data Catalog makes it easier for users to explore, discover, and access data intuitively—without relying on technical teams. ■ The ability to query data using natural language. ■ An audit trail with full lineage support for data processed both on- and off-premises. ■ Search by metadata, such as categories and tags ■ Automatic recommendations of relevant datasets and descriptions for ‘specific’ (sensitive) data.

CASE STUDIES

TOYOTA-ASTRA MOTOR

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 Thailand's PDPA law.

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 Thailand PDPA.

DNB is Norway's largest financial services group with 2.1 m customers in Norway alone. DNB was maintaining a highly complex data landscape, with more than 40 data sources, including multiple on-premises data warehouses such as Oracle and Teradata, and AWS data lake.

DNB

DNB is Norway's largest financial services group with 2.1 m customers in Norway alone. DNB was maintaining a highly complex data landscape, with more than 40 data sources, including multiple on-premises data warehouses such as Oracle and Teradata, and AWS data lake.

DNB developed a self-managed analytics ecosystem, fully deployed in AWS, called Insights Platform for Analytics (IPA), and integrated it with the Denodo Platform, to deliver mobile banking as well as advanced analytics use cases such as personalized pricing and better product recommendations.

The Denodo Platform provides a single point of controlled access to over 4,000 enterprise data warehouse views, 9 billion customer transactions, and digital clickstream data from DNB's digital channels.

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

The Denodo Platform seamlessly integrates many different systems at DNB **for GDPR "Right of access" reporting.**

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 devoted to churn prediction, fraud detection, and personalized pricing – while keeping the use of 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.

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

The Denodo Platform 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®

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.

> *"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

With Denodo, GetSmarter:

- Applied granular role- and attribute-based access controls
- Enabled data masking and anonymization for sensitive PII
- Created centralized audit trails and data lineage for compliance reporting
- Established a single semantic model to ensure consistent, trusted data views

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 Thailand's PDPA law, making the Denodo Platform 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 ensured that sensitive data was only accessed when explicitly authorized. These capabilities directly support key principles under Thailand's PDPA law, including consent-based processing, auditability, real-time access control, and data protection without unnecessary duplication.