Streamlining Compliance for Indonesia's Personal Data Protection Regulations

Today, Indonesia is the world's fourth most populous nation and the 10th largest economy in terms of purchasing power parity. A leader in Southeast Asia's digital economy, Indonesia's government has positioned the digital economy as a cornerstone of its broader economic development strategy.

In late 2022, the Indonesian government took an important step in unifying the country's data protection regulations, into the comprehensive Law No. 27 of 2022 on personal data protection (**"PDP Law"**). The PDP Law comprehensively addresses data ownership rights, restrictions on data usage, and the collection, storage, processing, and transfer of personal data belonging to Indonesian users. It applies to any entity that carries out legal actions in Indonesia, as well as to anyone conducting legal actions outside Indonesia if those actions have legal consequences within Indonesia or affect Indonesian Data Subjects (as defined in the law and explained below) residing abroad.

The PDP Law classifies personal data into two categories: general and specific. General personal data includes details like name, gender, nationality, religion, and marital status, carrying lower privacy risks. Specific personal data, considered more sensitive, includes health records, biometric and genetic data, criminal history, children's data, financial information, and other legally designated sensitive data. Due to higher privacy risks, processing specific data requires stricter regulatory compliance, including impact assessments and, in some cases, appointing a Data Protection Officer (DPO, as defined in the law), especially for large-scale operations or data related to criminal activity.

Key Roles Specified in the PDP Law

Data Subject: Individuals associated with Personal Data are known as **Data Subjects.** The PDP Law defines Personal Data as any information related to an individual, whether directly identified or identifiable when combined with other data, through electronic or non-electronic means.

Personal Data Controller: Defined in the PDP Law as any person, public body, or international organization acting individually or jointly in determining the goals for – and exercising control over – the processing of Personal Data.

Personal Data Processor: Refers to any person, public body, or international organization acting individually or jointly to process Personal Data on behalf of a Personal Data Controller. Further, since the Processor cannot determine the goals for – and exercise control over – the processing of Personal Data by itself, a Processor can only process Personal Data after being appointed by a Controller.

Data Protection Officer: An official or officer appointed by the Personal Data Controller and Personal Data Processor to carry out the Personal Data Protection function, who may come from within and/or outside the respective Personal Data Controller and/or Personal Data Processor entity.

SOLUTION
PDP Compliance

INDUSTRY
Applicable to all companies doing business with Indonesian 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.

Key Principles of the PDP Law

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

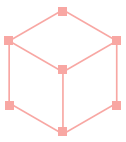
- **Lawfulness, Fairness, and Transparency:** Data must be handled legally, fairly, and transparently.
- **Purpose Limitation:** Data should only be collected for explicit, legitimate purposes and not further processed in a manner incompatible with those purposes.
- **Data Minimization:** Only data that is relevant and necessary for the purposes specified should be processed.
- **Accuracy:** Personal data must be kept accurate and up-to-date.
- **Integrity and Confidentiality:** Data must be processed securely, and it must protect against unauthorized or illegal processing and against accidental loss, destruction, or damage.

The PDP Law grants Data Subjects several rights, including the right to be informed about data collection and usage, as well as the right to access their data, correct inaccuracies, and request deletion when the data is no longer needed. They can also restrict or object to processing, especially in cases of direct marketing or automated decision-making. Individuals have the right to data portability, to withdraw consent at any time, and to exercise their rights without discrimination. Additionally, they can file complaints, seek legal remedies, and receive compensation if their data privacy is violated. Furthermore, the PDP Law mandates that data transfers to other jurisdictions can only occur under specific conditions, such as when the recipient country has equal or higher data protection standards. This can complicate operations for multinational companies, particularly those with centralized data processing centers outside Indonesia. Many organizations, especially small and medium-sized enterprises (SMEs), are not fully prepared for the law's requirements. They need to upgrade their data protection systems, create privacy policies, and enhance cybersecurity measures. Delaying these preparations can lead to significant penalties and a damaged reputation.

Indonesia's PDP Law and Data Management Challenges

- **Data Governance and Access Control:** Organizations must enable the lawful collection, processing, and storage of personal data, with clear **consent mechanisms** and governance policies.
- **Data Residency and Sovereignty:** Personal data must be stored within Indonesia, unless exemptions apply.
- **Security and Encryption:** Businesses must implement **encryption, data masking, and role-based access control (RBAC)** to safeguard personal data.
- **Consent and Purpose Limitation:** Data processing must be based on **explicit consent** from individuals and limited to specific purposes.
- **Right to Erasure and Data Portability:** Individuals have the right to request deletion of their personal data and obtain copies for transfer.

However, many enterprises struggle with **data silos, a lack of centralized governance, high data integration costs, and security vulnerabilities** across hybrid cloud and on-prem systems.



Limitations of Centralized Architectures for PDP Compliance

Many organizations have integrated lakehouse architectures as part of their broader data strategies, but lakehouses alone are not specifically designed to address **PDP Law compliance requirements.** While they offer scalability for analytics, they present key challenges in enabling effective **data governance, regulations tracking, and real-time access to sensitive data:**

- **Data Processing Delays:** Data lakehouses require data to be onboarded and transformed before becoming usable. This delay can impact compliance efforts that require real-time or near-real-time data access for governance, auditing, and reporting.
- **Hybrid and Multi-cloud Complexities:** PDP regulations require **controlled data sovereignty**, yet many organizations operate across multiple, often geographically distributed cloud systems. For these reasons, it can be inefficient and costly to manage compliance across **hybrid** environments using a data lakehouse alone.
- **Regulatory Burdens:** For regulatory compliance, businesses must **track and govern** data lineage, storage, transfers, and access. **Data lakehouses, on their own, lack compliance controls** for data tracking and regulatory audits.
- **Data Silos and Distributed Sources:** Some data will always reside outside of the data lakehouse, if only during mergers and acquisitions (M&A) activities or due to multi-cloud infrastructures. Replicating this distributed data into the data lakehouse using extract, transform, and load (ETL) processes increases operational complexity and cost.

Logical Data Management, with the Denodo Platform, for Seamless PDP 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.

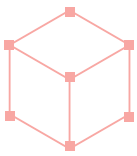
By embedding data governance and compliance in the same layer that delivers data to the business, companies can achieve compliance and manage risks across all data sources and silos, without sacrificing agility and competitiveness.

Unlike data lakehouses, which require data replication and ingestion before use, the **Denodo Platform provides real-time access to distributed data** while enabling full data **governance, security, and compliance** with the stringent requirements of PDP Law.

Semantic Unification of Data

The Denodo Platform provides a **business-friendly data layer** that integrates data from multiple sources, with unified semantics, **without the need for ETL processes**.

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. This makes compliance reporting **faster and more efficient.**



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, including hybrid and multi-cloud environments, 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 PDP 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.

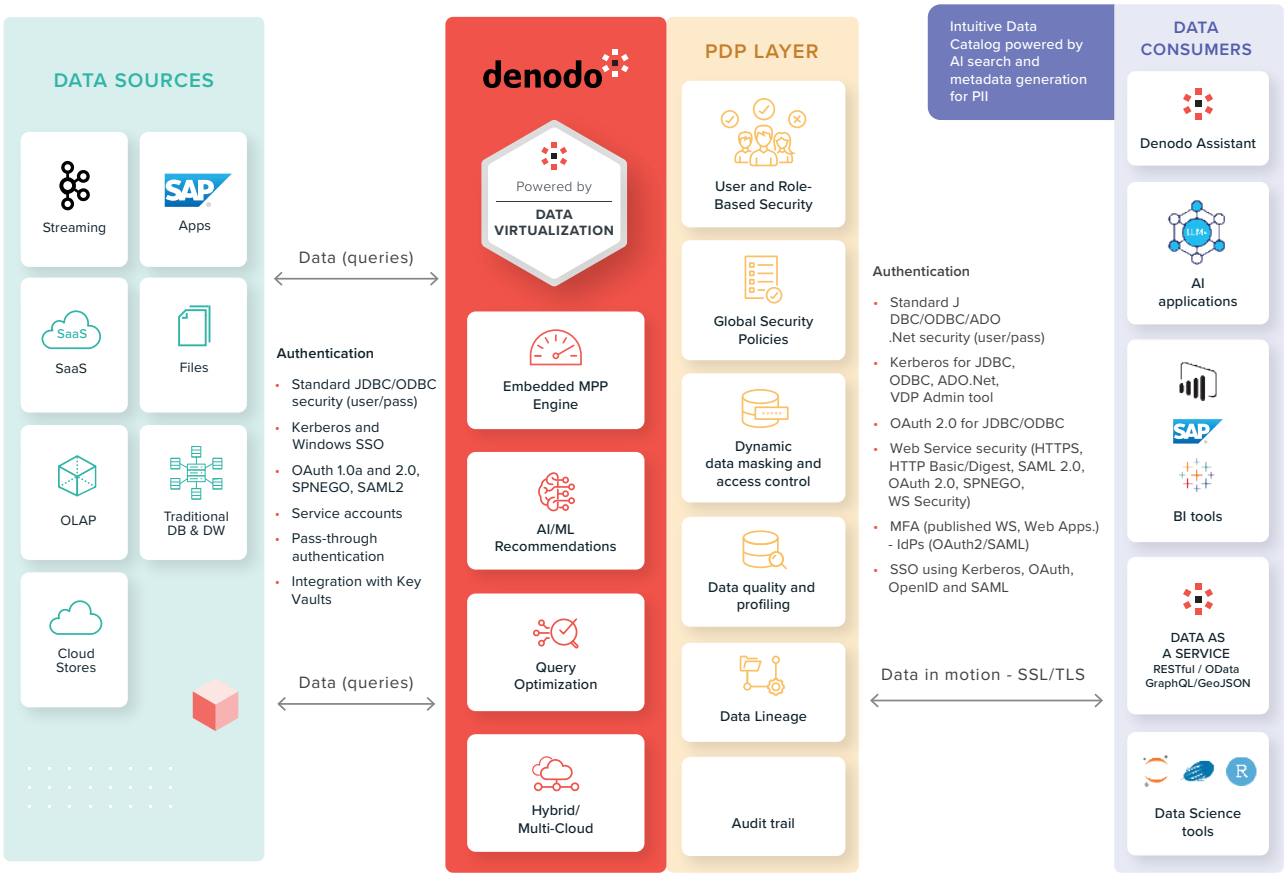
Role- and Attribute-Based Access Controls

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.

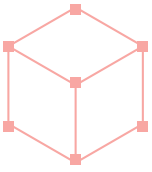
Global Policies

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 PDP.

How the Denodo Platform can Help Meet PDP 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, to recommend relevant datasets and even create AI-generated descriptions of views and columns – including those which contain sensitive information
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 ■ Search by metadata, such as categories and tags ■ Automatic recommendations of relevant datasets and descriptions for ‘specific’ (sensitive) data.



TOYOTA-ASTRA MOTOR

Toyota-Astra Motor (TAM) is the sole distributor of Toyota vehicles in Indonesia. It is currently the market leader in the Indonesian automotive industry, holding more than 30% market share. TAM is not only in the business of selling vehicles, but is also deeply involved in after-sales services for vehicle owners. On a day-to-day basis, TAM handles sensitive vehicle and owner information, making data protection and governance critical.

TAM had a fragmented data ecosystem, with data trapped in different business silos, causing significant data delivery challenges. The company wanted to simplify its complex data management landscape by removing traditional ETL and datamart bottlenecks, and it also wanted to establish more robust data governance and security practices.

TAM implemented the Denodo Platform, which seamlessly integrated several different source systems to create a logical data warehouse, and the company established a centralized access layer to boost data integrity and trust throughout the organization.

In addition to enhancing the resilience of TAM's supply chain and improving self-service analytics with strong governance and security controls, the Denodo solution provides TAM with real-time, comprehensive visibility into sales and service operations across territories. It also enabled user-activity auditing and real-time monitoring, fulfilling many of the requirements for compliance with PDP Law.

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

> *"The Denodo Platform has 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