Answering PDPL Challenges with IBM Solutions

How to implement PDPL at glance

IBM helps you to assess your existing environment to create best scenario PDPL solution framework

People

- Leadership Commitment
- Training and Awareness
- Privacy by Culture

Process

- Policies and Procedures
- Record of Processing Activity
- Data Protection Impact Assessment
- Third Party Risk Assessment
- Data Erasure, Disposal and Retention
- Trans Border Data Control
- Data Breach and Response
- Monitoring, Auditing and Continuous Improvement
- Data Subject Rights

Technology

- Data Discovery and Classification
- Data Access Control
- Risk & Compliance
- Data Breach & Response Management
- Consent Management System
- Data Subject Right

Critical Use Cases and Capabilities

Data Discovery & Classification

Data Access Control

Risk & Compliance

Data Breach & Response Management

Consent Management System

Data Subject Right

Use Case
Data Discovery & Classification

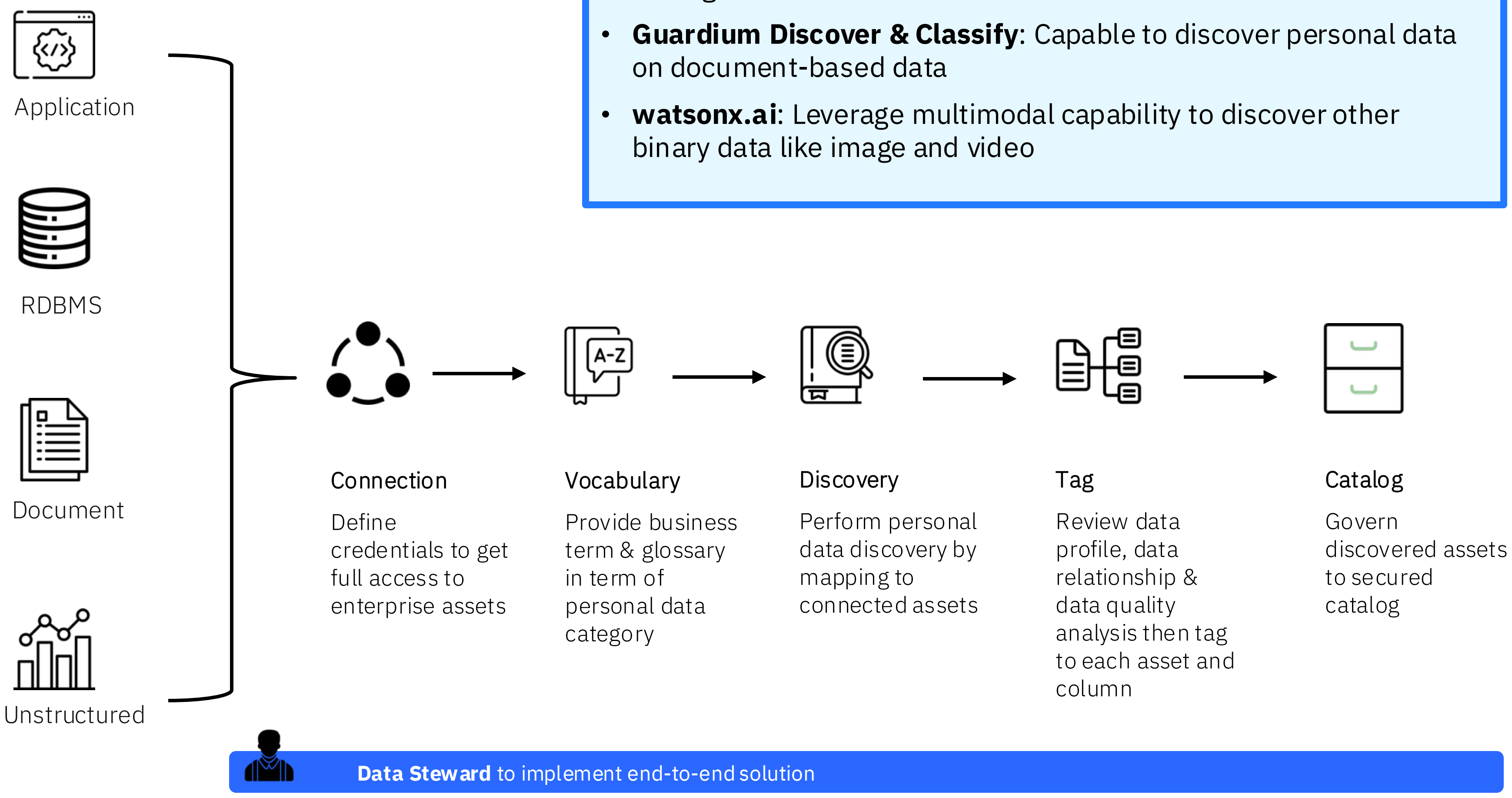
Provides industry vocabularies aligned to specific regulatory frameworks, with automation, data quality and lineage to lower the compliance mapping burden and enable trust in critical data

Capabilities

- Industry-Aligned Vocabularies
- Business Glossary
- Data Discovery
- Data Classification
- Automated Tag Management
- Data Quality Rules and Checks
- Relationship Explorer
- Catalogue

IBM Solution

- **IBM Knowledge Catalog**: Implement data governance in term of discovering structured data & cataloging, including policy management
- **Guardium Discover & Classify**: Capable to discover personal data on document-based data
- **watsonx.ai**: Leverage multimodal capability to discover other binary data like image and video



Connection

Define credentials to get full access to enterprise assets

Vocabulary

Provide business term & glossary in term of personal data category

Discovery

Perform personal data discovery by mapping to connected assets

Tag

Review data profile, data relationship & data quality analysis then tag to each asset and column

Catalog

Govern discovered assets to secured catalog

Data Steward to implement end-to-end solution

Use Case
Data Access Control

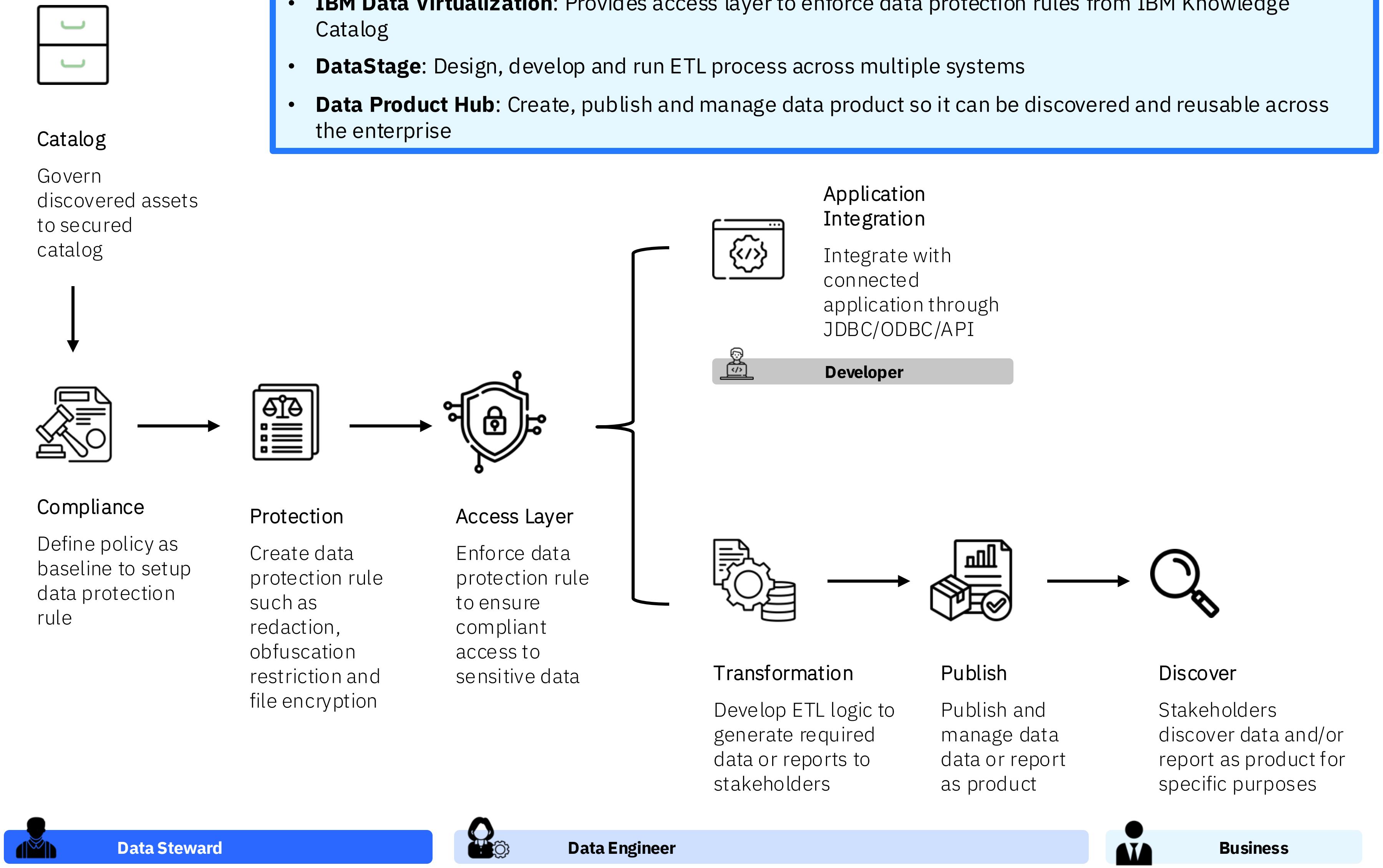
Enables secure, governed and seamless data delivery by enforcing protection rules through encryption and masking, building protected access layers to deliver trusted data products to stakeholders

Capabilities

- Virtualized Data Access
- API & BI Integration
- Access Control
- Data Transformation
- Parallel Processing
- Data Product Packaging
- Contract Management
- Usage Tracking

IBM Solution

- **IBM Knowledge Catalog**: Creates data protection rules through data masking and restriction
- **Guardium Encryption**: Perform file encryption to strengthen data protection
- **IBM Data Virtualization**: Provides access layer to enforce data protection rules from IBM Knowledge Catalog
- **DataStage**: Design, develop and run ETL process across multiple systems
- **Data Product Hub**: Create, publish and manage data product so it can be discovered and reusable across the enterprise



Catalog

Govern discovered assets to secured catalog

Compliance

Define policy as baseline to setup data protection rule

Protection

Create data protection rule such as redaction, obfuscation restriction and file encryption

Access Layer

Enforce data protection rule to ensure compliant access to sensitive data

Application Integration

Integrate with connected application through JDBC/ODBC/API

Transformation

Develop ETL logic to generate required data or reports to stakeholders

Publish

Publish and manage data or report as product

Discover

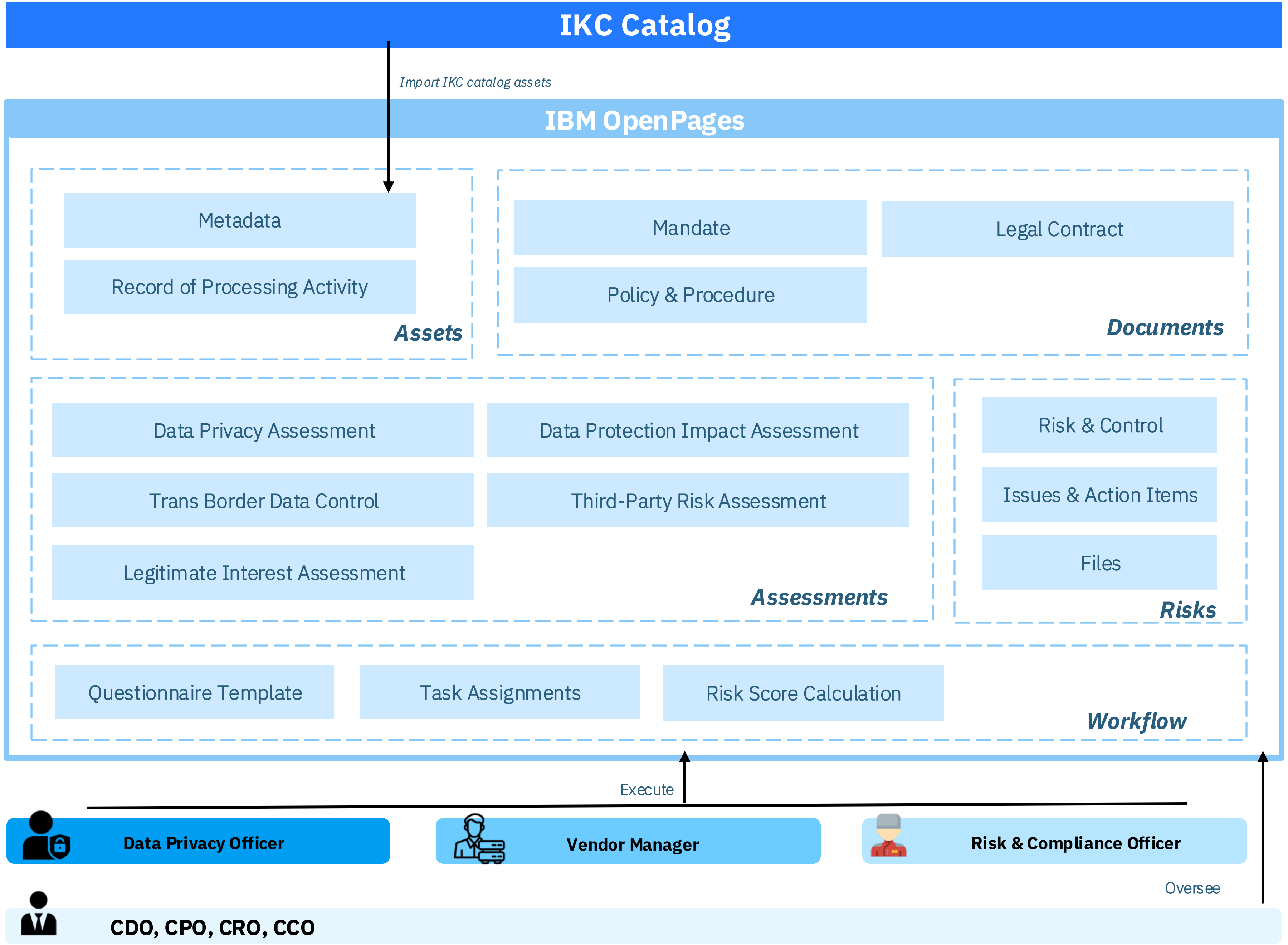
Stakeholders discover data and/or report as product for specific purposes

Use Case
Risk & Compliance

Automate personal data reporting to improve compliance accuracy, reduce audit time, and accelerate initiatives across organization

Capabilities

- Inventory Management
- Compliance Management
- Risk and Control Assessment
- Questionnaire Assessment
- Parallel Processing
- Data Product Packaging
- Automated Workflow
- Automated Asset Identification



IKC Catalog

Import IKC catalog assets

IBM OpenPages

Metadata

Record of Processing Activity

Assets

Mandate

Legal Contract

Policy & Procedure

Documents

Data Privacy Assessment

Data Protection Impact Assessment

Trans Border Data Control

Third-Party Risk Assessment

Legitimate Interest Assessment

Assessments

Risk & Control

Issues & Action Items

Files

Risks

Questionnaire Template

Task Assignments

Risk Score Calculation

Workflow

Execute

Data Privacy Officer

Vendor Manager

Risk & Compliance Officer

Oversee

CDO, CPO, CRO, CCO

Use Case
Data Breach & Response Management

Provides integrated solution that embeds data protection and monitoring with data access layer, automates reporting and stakeholder notifications, and centralize incident tracking for complete visibility and regulatory compliance

Capabilities

- Data Protection Rule
- Suspicious Activity Detection
- Threat Analytics
- Automated Response and Notification
- Risk Register
- Vulnerability Assessment

1 Prevent	2 Detect	3 Response	4 Evaluate
Protection Create data protection rule such as redaction, obfuscation restriction and file encryption	Alert Rule Create rule/policy to detect suspicious user activity when accessing certain database	Quarantine Quarantine suspicious user for specified period and send alert	Assess Perform vulnerability assessment to identify weakness on data protection implementation
Access Layer Enforce data protection rule to ensure compliant access to sensitive data	Report Monitor suspicious user activity by creating standard and custom report or dashboard	Notification Send notification to **regulator**, **data subject** and **related stakeholders** that are impacted by data breach incident	Incident Register Maintain log of data breach incidents includes what, when, where, who and how it happened and how it was resolved

IT Security

IBM Solution

- **IBM Knowledge Catalog + Guardium Encryption + IBM Data Virtualization** : Creates data access layer embedded with protection rules through data masking, restriction and file encryption
- **Guardium Data Protection + Vulnerability**: Create alert rule, suspicious report, quarantine alerted user, send notification to stakehodlers. It will also provide vulnerability assessment to identify weakness on data protection procedure
- **IBM OpenPages**: centralize data breach incident register in single repository

Use Case
Consent Management System

Provides a centralized way to capture and track user permissions, ensuring consent is purpose-based, timestamped, and easy to update or withdraw. It standardizes how data use is approved, maintains clear audit records, and helps organizations stay compliant while strengthening user trust.

Capabilities

- Capture and store purpose-based user consent
- Record timestamps and version history
- Allow easy updates or withdrawal of consent
- Enforce consent rules consistently across apps
- Maintain audit-ready logs for compliance

Why it matters

- PDP Law (UU 27/2022) requires organizations to capture, track, and prove valid consent.
- Without clear records timestamps, versions, and purpose-based approval companies risk fines, blocked marketing campaigns, regulator investigations, and significant loss of customer trust.

What it requires

- Purpose-based consent, clear opt-in/opt-out, timestamped and versioned consent text, easy withdrawal, and a centralized audit trail across all channels and systems.

Impact

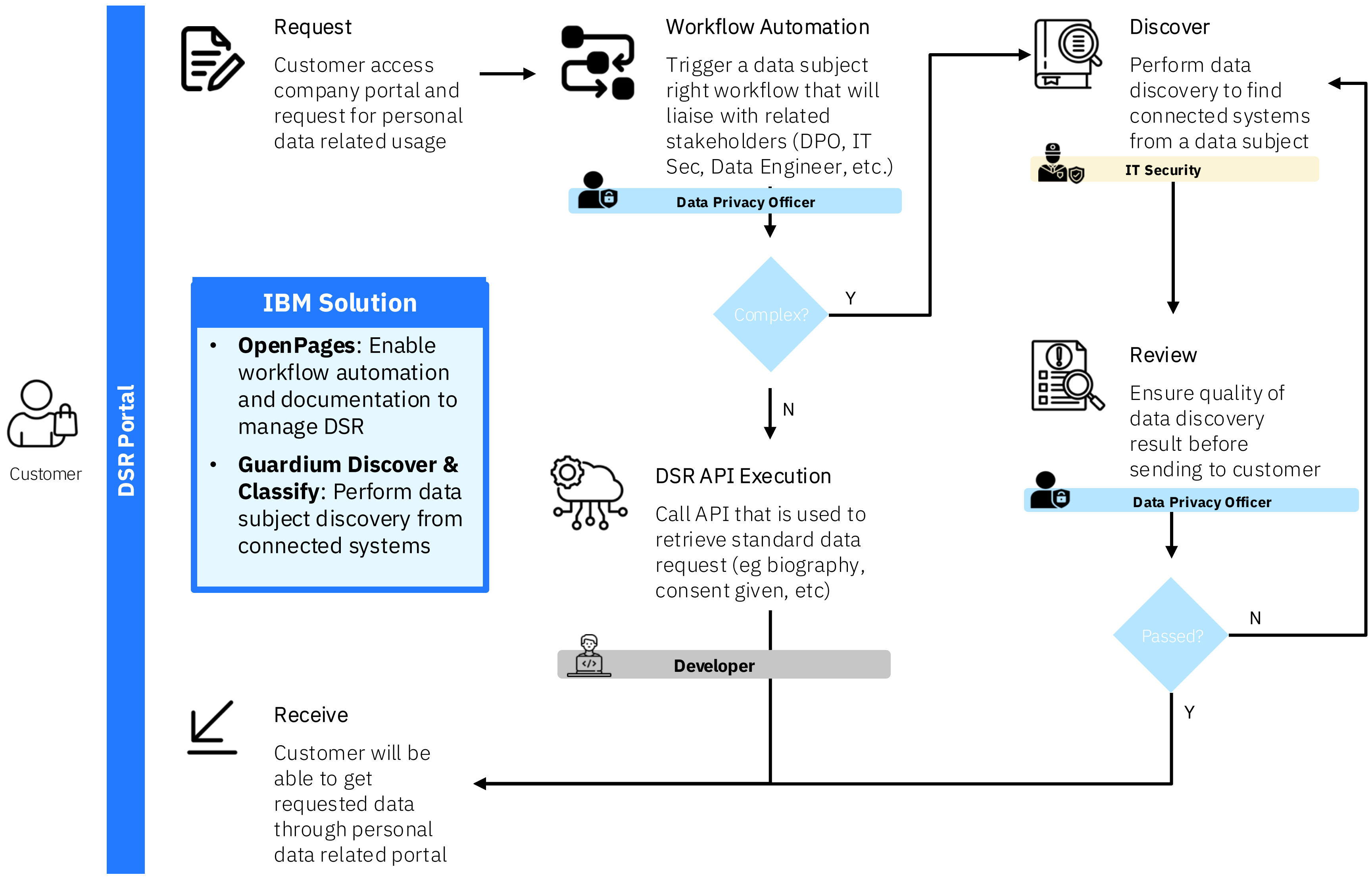
- Reduced regulatory risk, stronger customer trust, faster audits, and more confident and compliant personalization.

Use Case
Data Subject Right

Build a transparent and compliant data rights workflow aligned with PDPL, enabling customers to effortlessly exercise their right to know how their data is used

Capabilities

- Transparent Data Usage
- Regulatory Compliance
- Operational Efficiency
- Centralized Data Governance
- Customer Trust



Request

Customer access company portal and request for personal data related usage

Workflow Automation

Trigger a data subject right workflow that will liaise with related stakeholders (DPO, IT Sec, Data Engineer, etc.)

Data Privacy Officer

Discover

Perform data discovery to find connected systems from a data subject

IT Security

Review

Ensure quality of data discovery result before sending to customer

Data Privacy Officer

DSR API Execution

Call API that is used to retrieve standard data request (eg biography, consent given, etc)

Developer

Receive

Customer will be able to get requested data through personal data related portal

IBM Solution

- **OpenPages**: Enable workflow automation and documentation to manage DSR
- **Guardium Discover & Classify**: Perform data subject discovery from connected systems

IBM