

Answering PDPL Challenges with IBM Solutions

IBM

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

The IBM logo is displayed in white on a black rectangular background, positioned at the top left of the Technology section.

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

Legal Basis	IBM Solutions
<ul style="list-style-type: none">• Article 20 - 24, about consent management	<ul style="list-style-type: none">• Verify: Manage customer consent that captures consent creation and consent modification through entire customer lifecycle

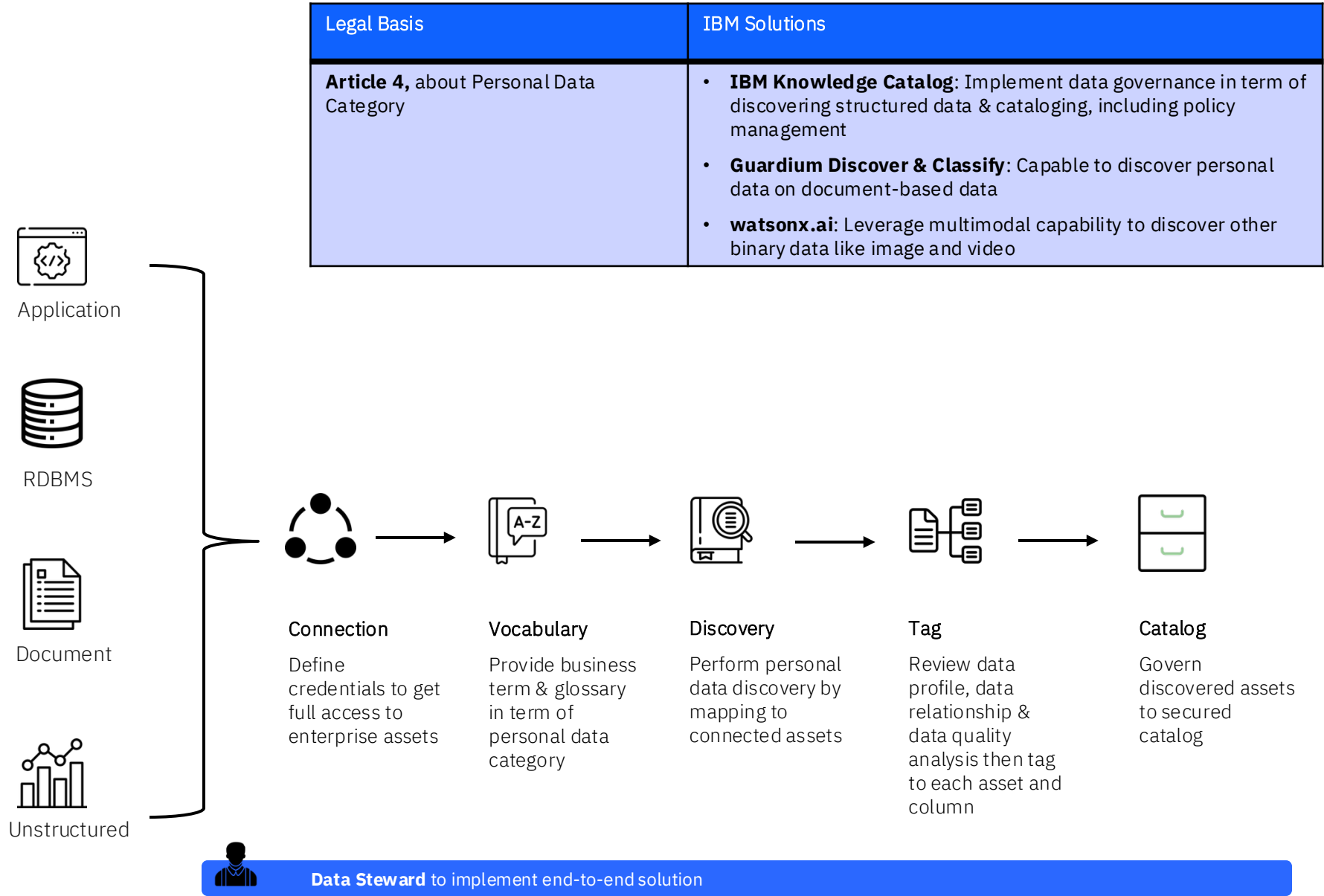
Use Case

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



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



Catalog

Govern discovered assets to secured catalog



Compliance

Define policy as baseline to setup data protection rule



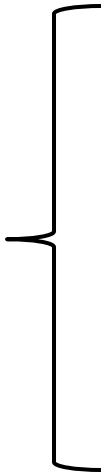
Protection

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

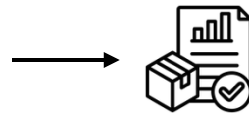


Developer



Transformation

Develop ETL logic to generate required data or reports to stakeholders



Publish

Publish and manage data data or report as product



Discover

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



Data Steward



Data Engineer



Business

Legal Basis	IBM Solutions
<ul style="list-style-type: none">• Article 35, about personal data security management• Article 36, 37, 38, 39, about personal data access control	<ul style="list-style-type: none">• 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

Use Case

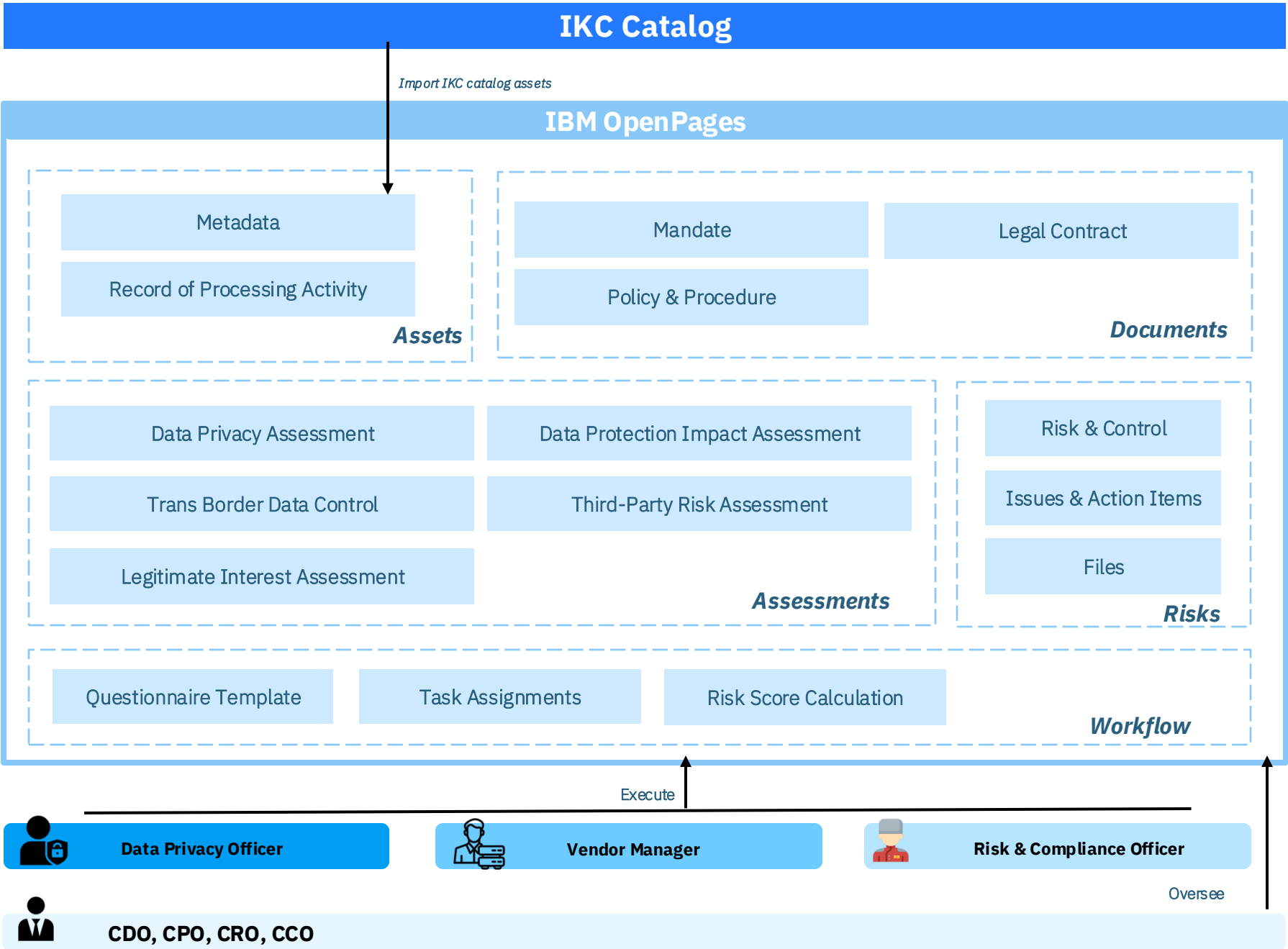
Risk & Compliance

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

Capabilities

- Risk and Control Assessment
- Questionnaire Assessment
- Automated Workflow
- Automated Asset Identification

Legal Basis	IBM Solutions
<ul style="list-style-type: none">• Chapter V, VI, VII, about personal data processing, obligation, personal data transfer	<ul style="list-style-type: none">• OpenPages: Governance, Risk and Compliance (GRC) tool to support documentation with intuitive user interface




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			
Legal Basis		IBM Solutions	
<ul style="list-style-type: none">• Article 16, 35, about personal data access control• Article 46, about data breach incident and response management		<ul style="list-style-type: none">• 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 stakeholders. 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.

Legal Basis	IBM Solutions
<ul style="list-style-type: none">• Article 20 - 24, about data subject right	<ul style="list-style-type: none">• OpenPages: Enable workflow automation and documentation to manage DSR• Guardium Discover & Classify: Perform data subject discovery from connected systems

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

Legal Basis	IBM Solutions
<ul style="list-style-type: none">• Article 5 - 15, about data subject right	<ul style="list-style-type: none">• OpenPages: Enable workflow automation and documentation to manage DSR• Guardium Discover & Classify: Perform data subject discovery from connected systems

