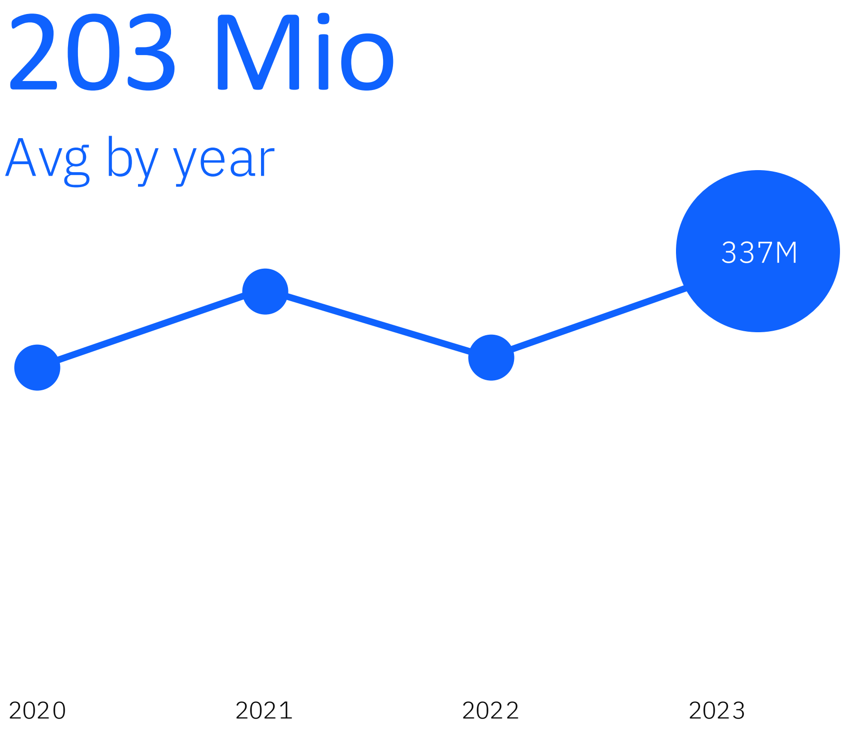
Navigating Indonesia’s Personal Data Protection Law (UU PDP No. 27/2022) with IBM Solutions

Data breaches growing in Indonesia society

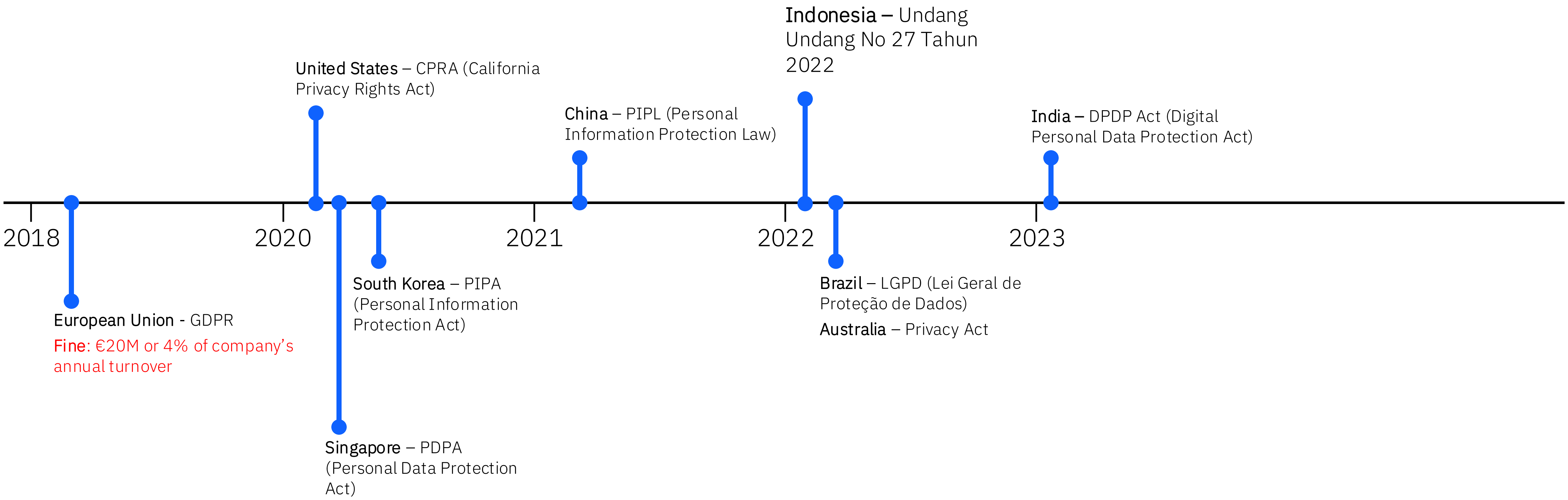
Report states that records of data exposed from data breach incidents increases in last 4 years



Average number of records exposed from major data breach cases in Indonesia from 2020 to 2023

From 2020 to 2023, Indonesia faced **major data breaches** across critical sectors: an e-commerce platform leak exposing **user accounts**, a health insurance breach with **sensitive data** sold on the **dark web**, a **voter database** hack by “Bjorka,” and a massive **leak of population and family records** by BreachForums. These incidents revealed severe weaknesses in national data protection.

Timeline of Amendments of Global Data Protection Regulations at a Glance



European Union - GDPR

Fine: €20M or 4% of company's annual turnover

United States – CPRA (California Privacy Rights Act)

Singapore – PDPA (Personal Data Protection Act)

South Korea – PIPA (Personal Information Protection Act)

China – PIPL (Personal Information Protection Law)

Indonesia – Undang Undang No 27 Tahun 2022

Brazil – LGPD (Lei Geral de Proteção de Dados)

Australia – Privacy Act

India – DPDP Act (Digital Personal Data Protection Act)

GDPR introduces key concepts related to Personal Data Privacy

Data Subject

- Consumer
- Employee
- Outsource
- Staff under vendor
- Other Parties

The data subject presents all the parties to which personal data may be involved

GDPR Main Focus

1 Personal Data

2 Data Protection

3 Data Subject Rights to:

(i) Request Information

(ii) Access

(iii) Revise

(iv) Delete

(v) Processing Limitation

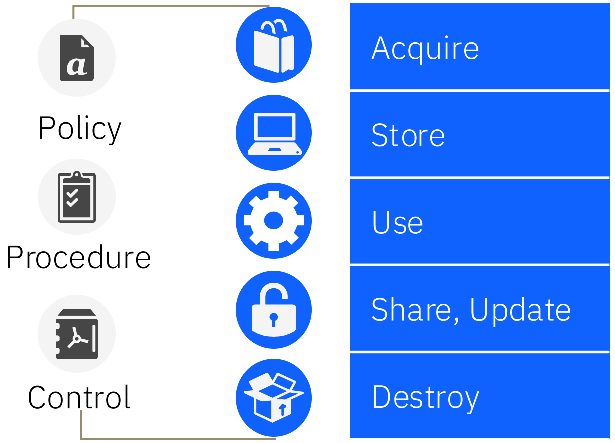
(vi) Data Portability

(vii) Data Priorities

(viii) Not subject to automated decision making

Processing Scope

Processing is any **activity or series of activities** performed **on the person of the data owner** or on the collection of personal data, whether **automatic or not**, including:


Policy

Procedure

Control

- Acquire
- Store
- Use
- Share, Update
- Destroy

Processing Principal

The GDPR establishes principles in the processing of personal data to ensure that it is done to protect data subjects.

Briefly, these principles stipulate that personal data must:

- Legitimacy, fairness, and transparency
- Objective restriction
- Minimalize data
- Accuracy
- Storage restrictions
- Integrity and secrecy (security)
- Accountability

In particular, the GDPR also establishes the basis for processing to be considered legal, namely:

- Consent
- Contract
- Legal obligations
- Public duty
- Legitimate interest

Indonesia Personal Data Protection Law (PDPL)

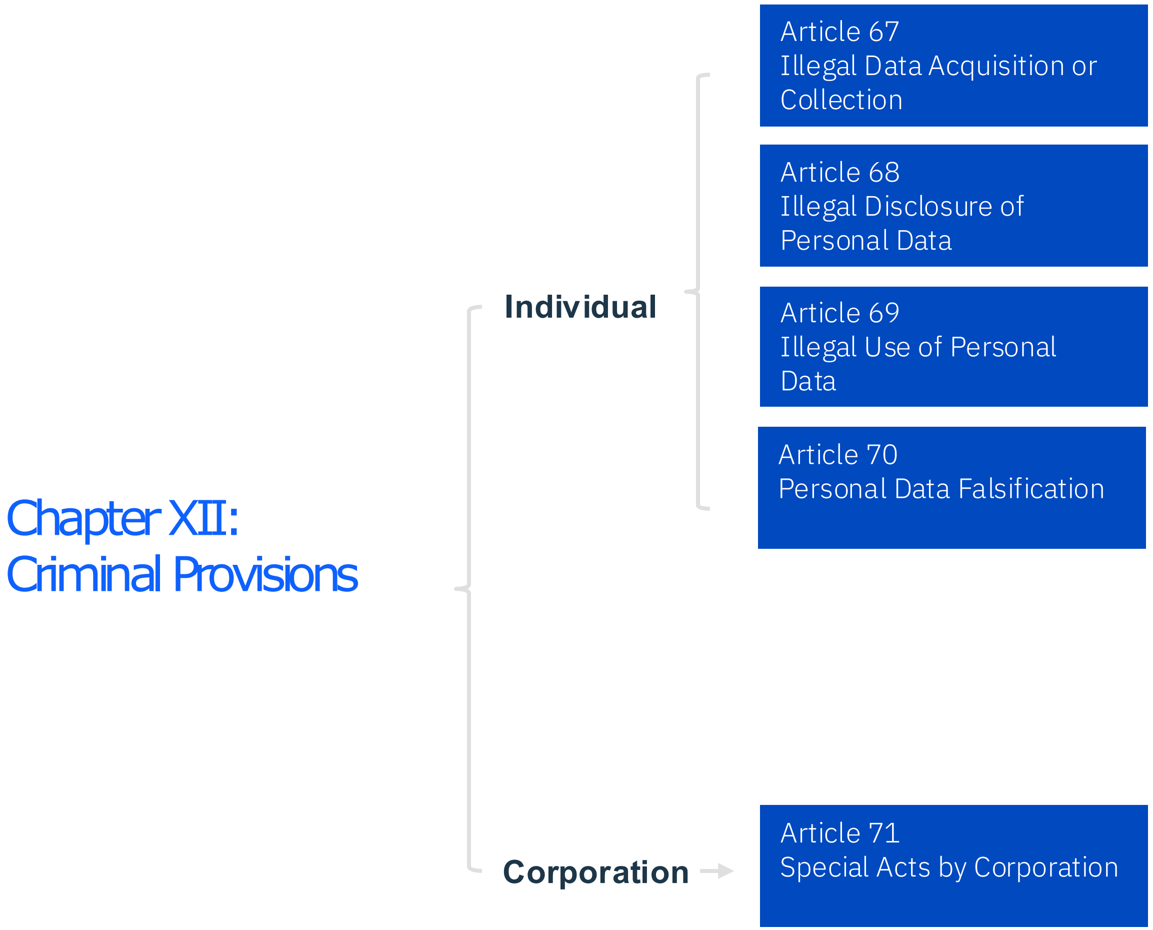
Undang Undang No 27 Tahun 2022

Chapter I: General Provisions	Chapter II: Types of Personal Data	Chapter III: Rights of Personal Data Subjects	Chapter IV: Processing of Personal Data	Chapter V: Obligations of Personal Data Controllers
Chapter VI: Personal Data Processors	Chapter VII: International Cooperations	Chapter VIII: Personal Data Protection Supervisor Authority	Chapter IX: Public Participation	Chapter X: Dispute Resolution and Procedural Law
Chapter XI: Prohibitions in Personal Data Processing	Chapter XII: Criminal Provisions	Chapter XIII: Administrative Provisions	Chapter XIV: Transitional Provisions	Chapter XV: Closing Provisions

Personal Data is any data about a **person** either identified and/or can be identified separately or in combination with other information either directly or indirectly through **electronic** and/or **non-electronic** systems.

Elucidation of Indonesia PDPL Criminal Sanctions

Criminal sanctions under Indonesia Personal Data Protection Law (PDPL) underscore the seriousness of violations with penalties



Chapter XII: Criminal Provisions

Individual

Article 67
Illegal Data Acquisition or Collection

Article 68
Illegal Disclosure of Personal Data

Article 69
Illegal Use of Personal Data

Article 70
Personal Data Falsification

Corporation

Article 71
Special Acts by Corporation

~6 yrs

Individual can get a maximum prison sentence by intentionally and unlawfully creates false personal data

~Rp 6B

..and/or a maximum fine can be added

~Rp 100B

Sanctions will be imposed on the management, the person giving the order, or the policy maker.

Key Processes Required by Indonesia PDPL

Personal Data Protection Law aimed at guaranteeing the right of citizens to personal protection and raising public awareness of data privacy

Chapter II

Data Discovery & Classification

Personal Indefinable Information:

- Health data and information
- Biometric data
- Genetic data
- Crime record
- Personal financial data
- Full name
- Gender
- Citizenship
- Religion
- Marital status
- Personal Data combined to identify a person.
- Other data in accordance with the provisions of the legislation.

Chapter III

Data Subject Rights

Erasure, Disposal and Retention

Mandatory Elements:

- Customer Contact Point
- Request Ticketing Platform

Chapter IV

Consent Management

Mandatory Elements:

- Consent Management Platform

Chapter V

Policies and Procedures

Data Breach Management

Legitimate Interest Assessment

Chapter VI

Record of Processing Activity

Access Control

Data Encryption & Masking

Third Party Risk Assessment

Data Protection Impact Assessment

Independent Department

Terminologies

Data Controller

Determining the purpose of data processing and performing control over data processing activities.

Data Processor

Processing personal data on behalf of the Data Controller..

Data Privacy Officer

Continuously and systematically monitoring of personal data on a large scale or related to criminal data.

Chapter VII

Trans-Border Data Control

Chapter XIV

Training and Awareness

Who are the personas

Understand the different perspectives!

DPO

Data Privacy Officer

- Oversee internal compliance
- Liaison with PDPL authorities
- Advise on data processing
- Manage data breach reporting

Data Management

Data Engineer and Data Governance (Steward)

- Conduct data inventory and mapping
- Determine personal data classification
- Manage data lifecycle
- Support data data subject rights

App Dev and IT Sec

Application Developer and IT Security

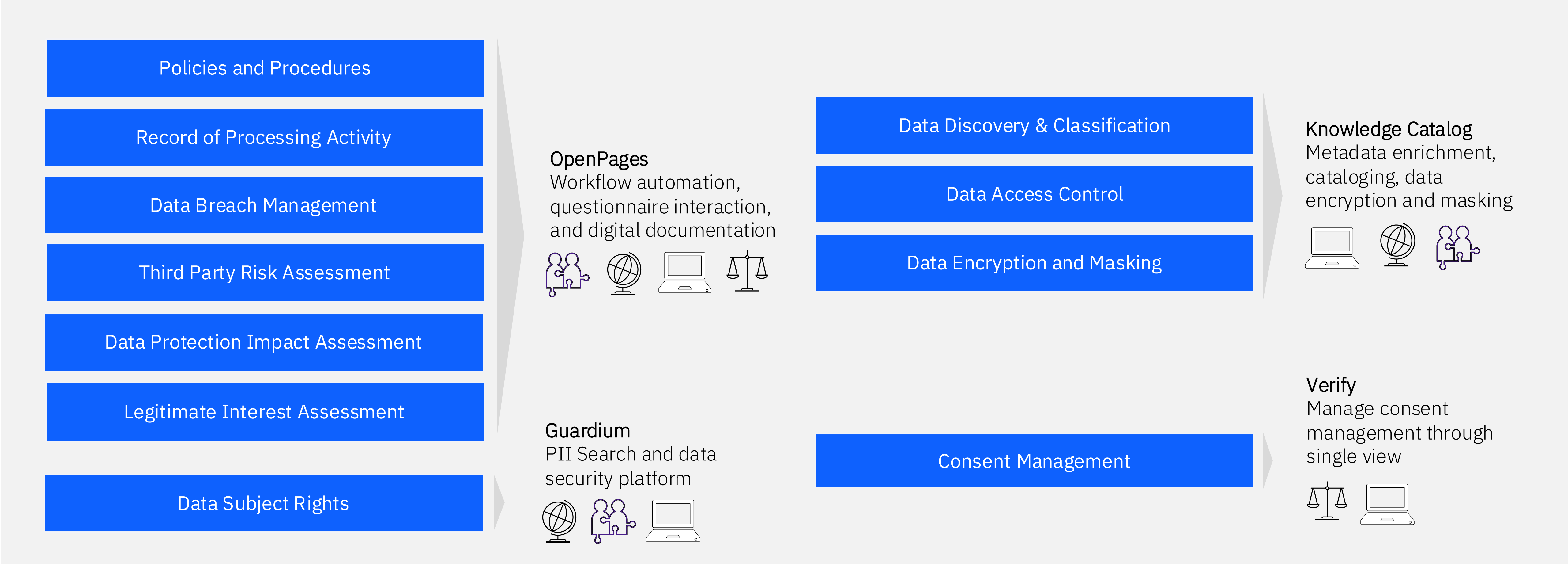
- Technical implementation of data protection
- Developing and testing incident response plans
- Monitoring data breaches and incident notification
- Implement consent and terms at application
- Develop customer contact point to enable data subject rights

Risk and Compliance

Legal, Compliance, Audit and Risk Management

- Create data processing contracts
- Manage consent management mechanisms and privacy policies
- Conduct compliance audits
- Enable risk management related to personal data

IBM Solution for PDPL Compliance



- Policies and Procedures
- Record of Processing Activity
- Data Breach Management
- Third Party Risk Assessment
- Data Protection Impact Assessment
- Legitimate Interest Assessment

OpenPages
Workflow automation, questionnaire interaction, and digital documentation
🧩 🌐 💻 ⚖

- Data Subject Rights

Guardium
PII Search and data security platform
🌐 🧩 💻

- Data Discovery & Classification
- Data Access Control
- Data Encryption and Masking

Knowledge Catalog
Metadata enrichment, cataloging, data encryption and masking
💻 🌐 🧩

- Consent Management

Verify
Manage consent management through single view
⚖ 💻

- Erasure, Disposal and Retention
- Trans-Border Control

Need further assessment to conclude

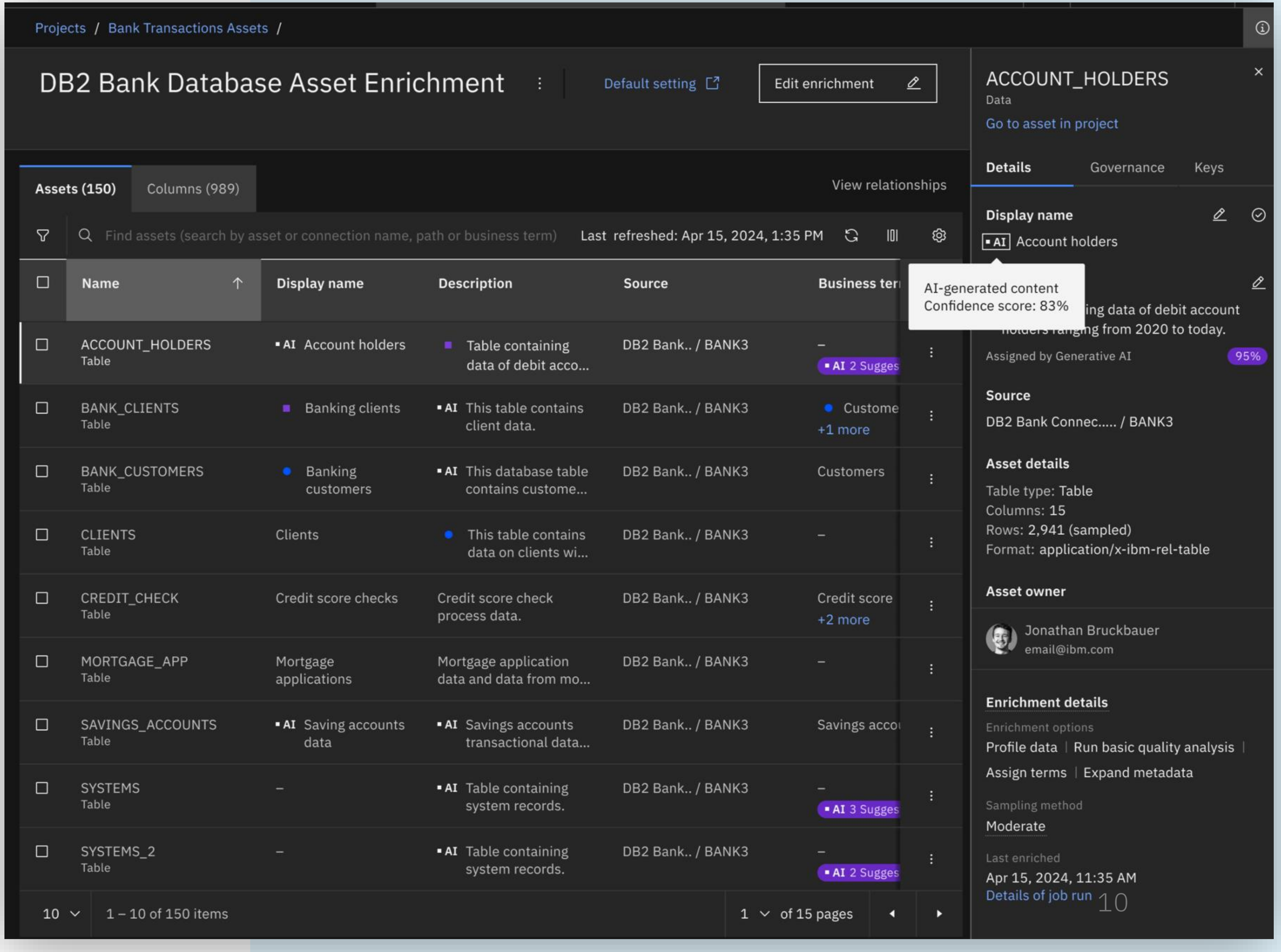
Key Persona

⚖ LR&C 🌐 Data 💻 IT 🧩 DPO

Metadata Enrichment in IKC to identify business terms laid on data

Key Features

- Automatically **generate meaningful column names** and descriptions with context
- **Assign terms** based on semantic meaning and context
- **Improved precision of term assignments** with best-in-class automation & accuracy that doubles the number of correct column mappings (reduction in false positives)
- **Accelerate data curation** through increased accuracy and precision of auto-term assignments using AI and trusted LLMs from IBM Research
- Provide Gen AI capabilities to other Data & AI products



Projects / Bank Transactions Assets /

DB2 Bank Database Asset Enrichment

Last refreshed: Apr 15, 2024, 1:35 PM

□	Name	Display name	Description	Source	Business ter
□	ACCOUNT_HOLDERS Table	▪ AI Account holders	▪ Table containing data of debit acco...	DB2 Bank.. / BANK3	– ▪ AI 2 Sugges
□	BANK_CLIENTS Table	▪ Banking clients	▪ AI This table contains client data.	DB2 Bank.. / BANK3	● Custome +1 more
□	BANK_CUSTOMERS Table	● Banking customers	▪ AI This database table contains custome...	DB2 Bank.. / BANK3	Customers
□	CLIENTS Table	Clients	● This table contains data on clients wi...	DB2 Bank.. / BANK3	–
□	CREDIT_CHECK Table	Credit score checks	Credit score check process data.	DB2 Bank.. / BANK3	Credit score +2 more
□	MORTGAGE_APP Table	Mortgage applications	Mortgage application data and data from mo...	DB2 Bank.. / BANK3	–
□	SAVINGS_ACCOUNTS Table	▪ AI Saving accounts data	▪ AI Savings accounts transactional data...	DB2 Bank.. / BANK3	Savings accou
□	SYSTEMS Table	–	▪ AI Table containing system records.	DB2 Bank.. / BANK3	– ▪ AI 3 Sugges
□	SYSTEMS_2 Table	–	▪ AI Table containing system records.	DB2 Bank.. / BANK3	– ▪ AI 2 Sugges

10 ⌄ 1 – 10 of 150 items

1 ⌄ of 15 pages

AI-generated content
Confidence score: 83%

ACCOUNT_HOLDERS
Data
Go to asset in project

Display name
▪ AI Account holders

ing data of debit account holders ranging from 2020 to today.
Assigned by Generative AI 95%

Source
DB2 Bank Connec..... / BANK3

Asset details
Table type: Table
Columns: 15
Rows: 2,941 (sampled)
Format: application/x-ibm-rel-table

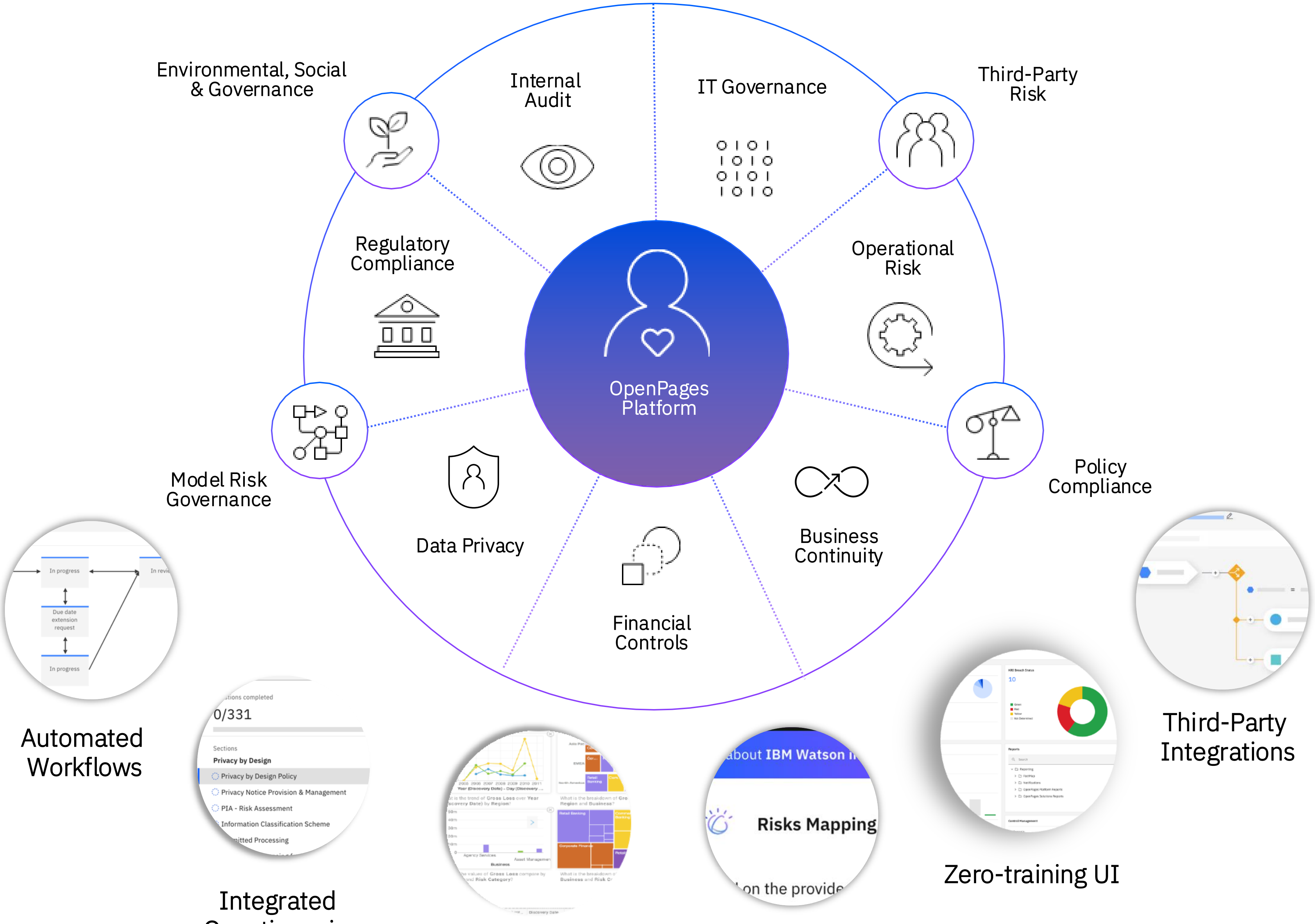
Asset owner
Jonathan Bruckbauer
email@ibm.com

Enrichment details
Enrichment options
Profile data | Run basic quality analysis | Assign terms | Expand metadata

Sampling method
Moderate

Last enriched
Apr 15, 2024, 11:35 AM
Details of job run

Transform the way risk and compliance professionals work with IBM OpenPages



stions completed

0/331

Sections

Privacy by Design

- Privacy by Design Policy
- Privacy Notice Provision & Management
- PIA - Risk Assessment
- Information Classification Scheme
- mitted Processing

Automated Workflows

Integrated Questionnaire

Predictive Insights

Expertise with AI

Zero-training UI

Third-Party Integrations

Protect Data, Simplify Compliance

Guardium Discover and Classify

IBM Guardium
Discover & Classify

Highly accurate discovery and classification of structured and unstructured data

Comprehensive Discovery

Automatically detect known and unknown sensitive data across hybrid environments, whether at rest, in motion, or in overlooked data sources

Business-Driven Tagging

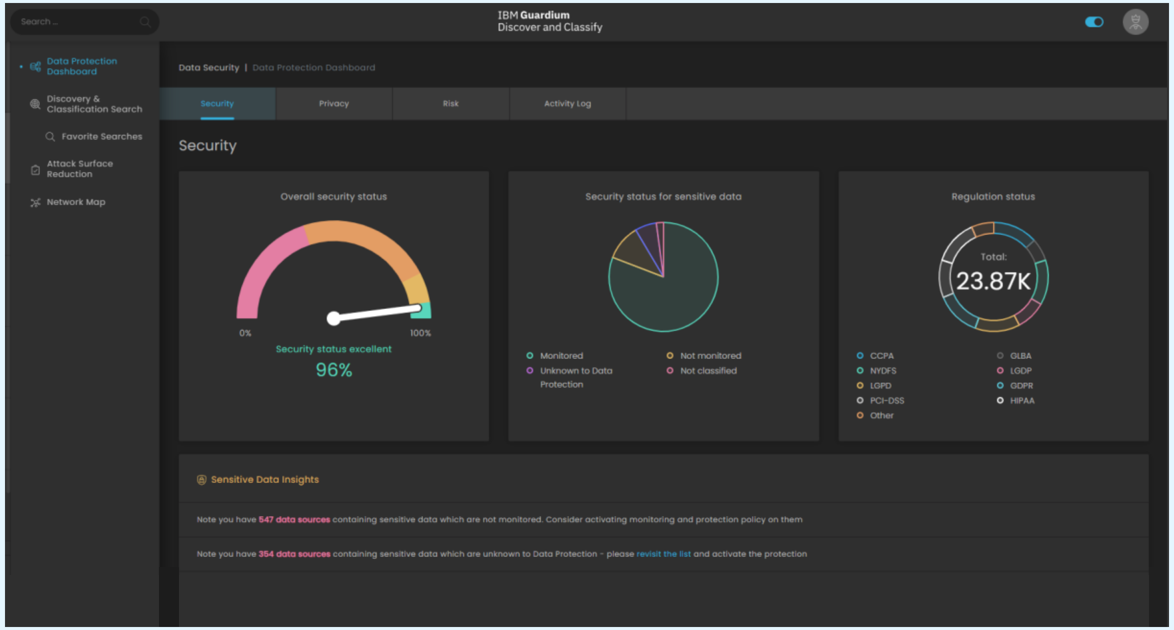
Enrich existing security and compliance tools with deep data-level context to enable smarter protection and better prioritization of defenses

Accurate Classification

Industry-leading classification accuracy for both structured and unstructured data using AI and contextual machine learning, which is verified by independent tests

Contextualized Insights

Reveal the business context of sensitive data, like a European citizen’s credit card residing in a US data center without GDPR controls, to highlight true risk and trigger the correct response



Note you have 547 data sources containing sensitive data which are not monitored. Consider activating monitoring and protection policy on them

Note you have 354 data sources containing sensitive data which are unknown to Data Protection - please revisit the list and activate the protection

99.7%

accuracy in data classification according to independent testing, assuming 80% of business data is unstructured

Financial Services Provider, US

Facing fragmented tools and increasing regulatory pressure, the organization needed a unified approach to data security and privacy. Guardium Discover and Classify delivered this at scale, scanning 3,000 databases in two weeks, and integrated seamlessly with existing tools. The solution streamlined audit readiness, cut DSAR response times from days to minutes, and gave business units self-service access to trusted data insights.

Unlock identities and enable more effective communications throughout the organization with IBM Security Verify

Admin user activity

- User activity dashboards
- Custom reporting
- Webhook/CRM integrations
- Marketing process workflow
- Identify fraudulent users

Build on a robust platform

- Scale and availability
- Standards and compliance
- Admin and dev tooling
- API driven & customizable
- Event monitor, log, & stream

IBM **Security Verify**

Capture / Engage with users

- Registration & profiling
- SSO / MFA / Risk authN
- Password-less authN
- Social login
- Custom branding

Manage users and artifacts

- Profile management and admin
- Data privacy and consent
- User governance
- Account relationship and linking
- Attribute mapping

Understand where your state and how you implement PDPL

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
- Documentation and Recordkeeping
- Data Encryption and Masking
- Data Access Control
- Consent Management Platform
- Data Request Automation
- Automated Workflow

IBM