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

Data breaches on the rise in Indonesia society

BreachForums users Björka uploaded billions of personal data that was claimed to be the result of breaking into corporate sites to state institutions in 2 months

91 million Tokopedia customer data, breached April 2020, uploaded August 19, 2022.

17 million State Electricity Company (PLN) customer data leakage on August 19, 2022

270 million Wattpad social media user data was uploaded on August 20, 2022. This data was compromised in June 2020.

26 million IndiHome subscriber data, uploaded on 20 August 2022.

1.3 billion SIM card data leakage from the Ministry of Communication and Information (Kominfo) found on September 1, 2022

105 million population data from the General Elections Commission (KPU), uploaded on September 6, 2022.

[1] "INFOGRAPHIC: Björka 'Achievements' Series". CNN Indonesia. September 15th, 2022.

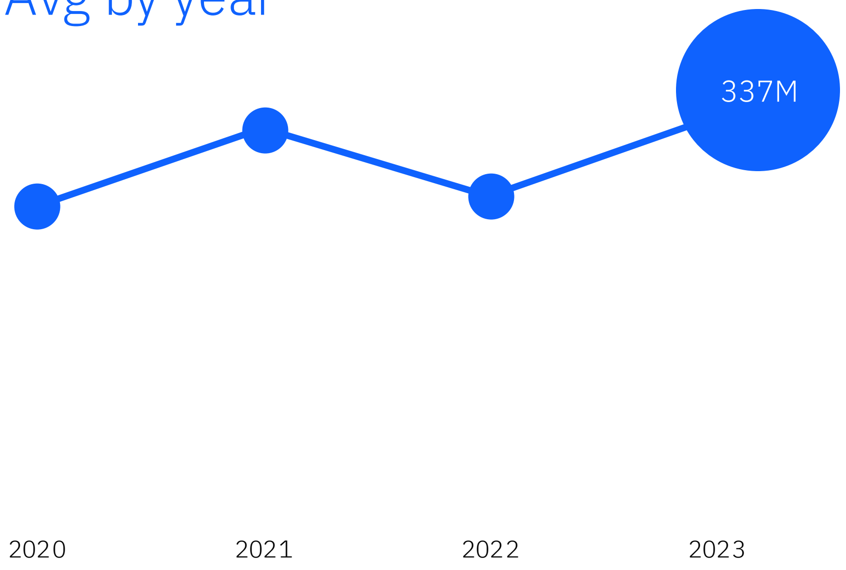
[2] "What is Breached Forums Involved in 4 Cases of Data Leaks in Indonesia in the Last Month?". KOMPAS.com. August 07th, 2022.

Data breaches growing in Indonesia society

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

203 Mio

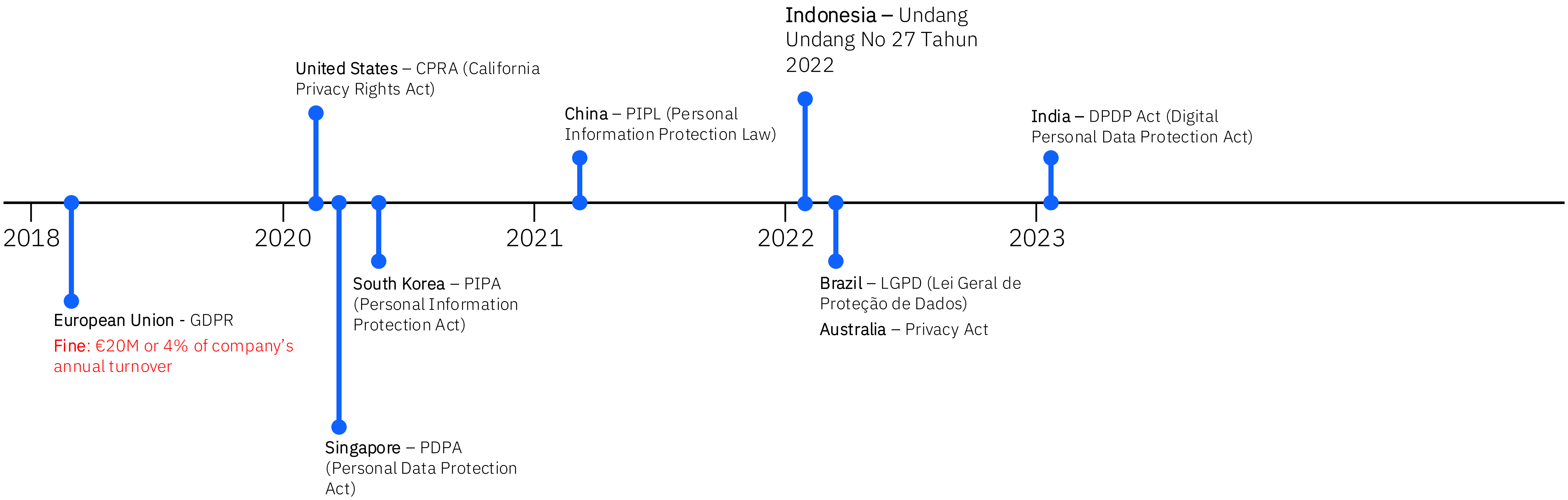
Avg by year



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

CALIFORNIA PRIVACY RIGHTS ACT

PIPA South Korean Personal Information Protection Act

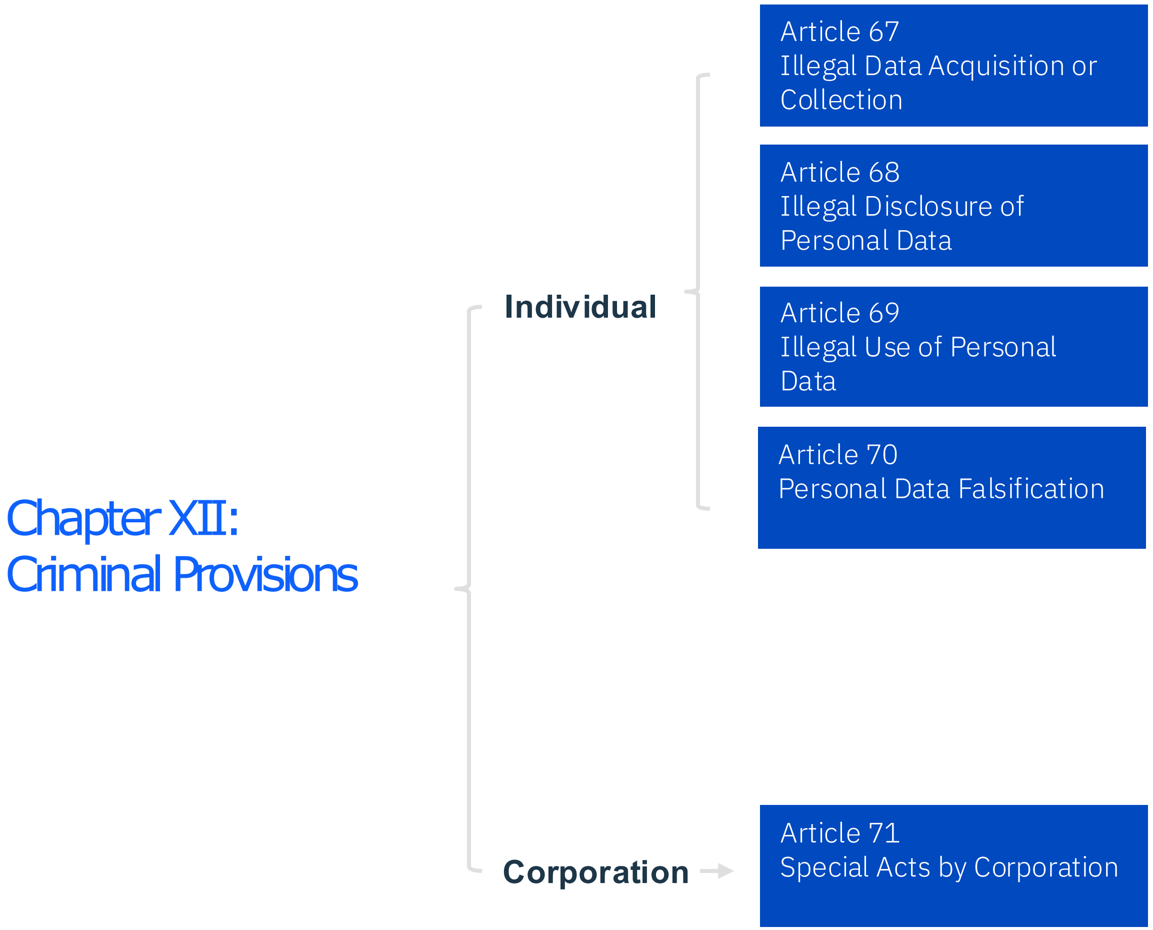
China's PIPL

LGPD Lei Geral de Proteção de Dados

DPDP ACT

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.

Indonesia parliament passes long-awaited Data Protection Bill

Personal Data Protection Law aimed at guaranteeing the right of citizens to personal protection and raising public awareness of data privacy with 2 years transition period given

- Personal Data Types
- Data Owner Rights
- Processing of Personal Data
- Exception
- Controller / Processor Roles
- Data Protection Officer
- Personal Data Transfer
- International Cooperation
- Sanction / Penalty

Terminologies

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.

Data Protection Authority is the national body established to be responsible for upholding the rights of individuals to the protection of their personal data through the enforcement and monitoring of compliance with local data privacy laws.

Data Controller is defined as any person, public body, or international organization that acts individually or jointly in determining the purpose of data processing and performing control over data processing activities.

Data Processor is defined as any person, public body, and international organization acting individually or jointly in processing personal data on behalf of the Data Controller.

Data Protection Officer (DPO) is mandatory for organizations that process personal data for public interests, main activities involve the continuous and systematic monitoring of personal data on a large scale or related to criminal data.

Sanction / Penalty

- **6 years** imprisonment and/or a fine of **IDR 6 billion** maximum for falsifying personal data (Article 68).
- **5 years** imprisonment and/or a fine of **IDR 5 billion** for collecting or using personal data that do not belong to them (Article 67).
- **4 years** imprisonment and/or a fine of **IDR 4 billion** for disclosing data that do not belong to them (Article 67).
- **10 times** fine for Corporate (Article 70).

[1] "INFOGRAPHIC: Personal Data Protection Bill to Anticipate Data Misuse". MOCI. September 9th, 2019.

[2] "Contents of the Personal Data Protection Law: Prohibitions, Sanctions and Types of Data". Detik News. September 20th, 2022.

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.

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

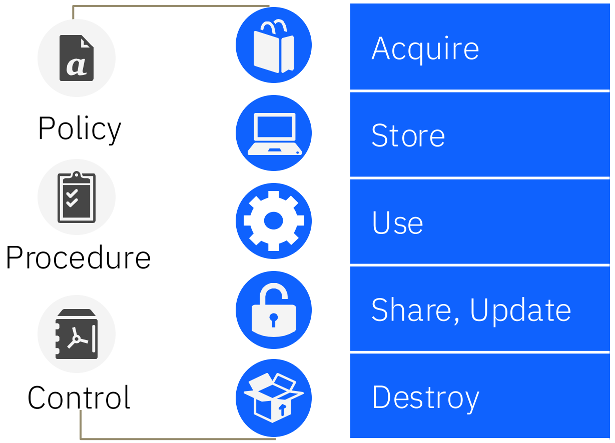
(vi) Data Portability

(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:



Processing Principal

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

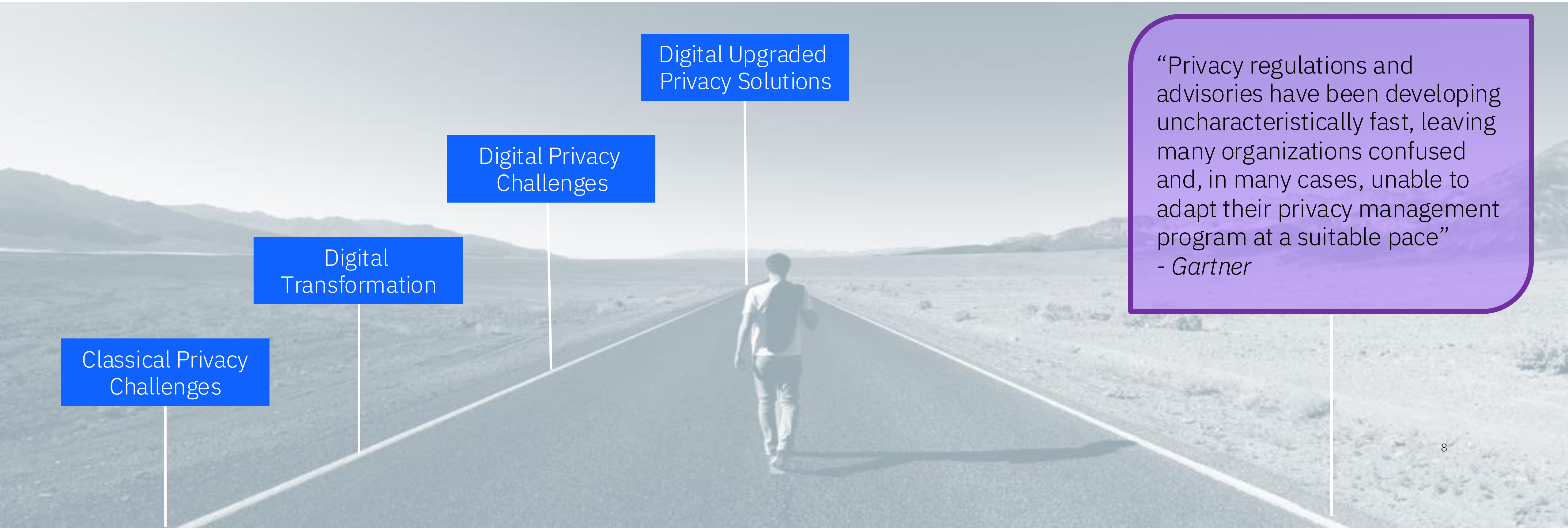
Briefly, these principles stipulate that personal data must:

- 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

Privacy Compliance is a continuous Journey, not a Destination!


Classical Privacy Challenges
Digital Transformation
Digital Privacy Challenges
Digital Upgraded Privacy Solutions
8

> “Privacy regulations and advisories have been developing uncharacteristically fast, leaving many organizations confused and, in many cases, unable to adapt their privacy management program at a suitable pace”
> \- *Gartner*

Our story understands and follows the client‘s privacy journey!

Why privacy should be a key priority?

#1 Intensive Globalization

Due to continued interaction between nations, organizations, people and businesses our society and economy have become global a data centric, in which the personal data of individuals travels beyond borders thus privacy should be a priority for all.

#2 Technology Digitalization

The new digital solutions, cutting-edge technologies drive organizations to become more effective, by supporting their decision-making process to gain insights into the datasets, collected on clients and/or generated by their overall business activities.

#3 Pervasiveness & Sensitivity

The growth of the global data sphere, the growing pervasiveness of digital technologies, the increase of data incidents, breaches has made clients customers, data subjects (employees, consumers) even more sensitive to the ever-changing, cumulative, and exponential privacy risk landscape.

#4 Increased Regulation

Privacy is a human right and has become a focus for many regulators to create the applicable privacy laws throughout the world to ensure such fundamentum to individuals when controllers, processors, third parties collect, store, transfer, etc. their personal data. As of 2020 there are 148 different privacy laws.

#5 Global Privacy Governance

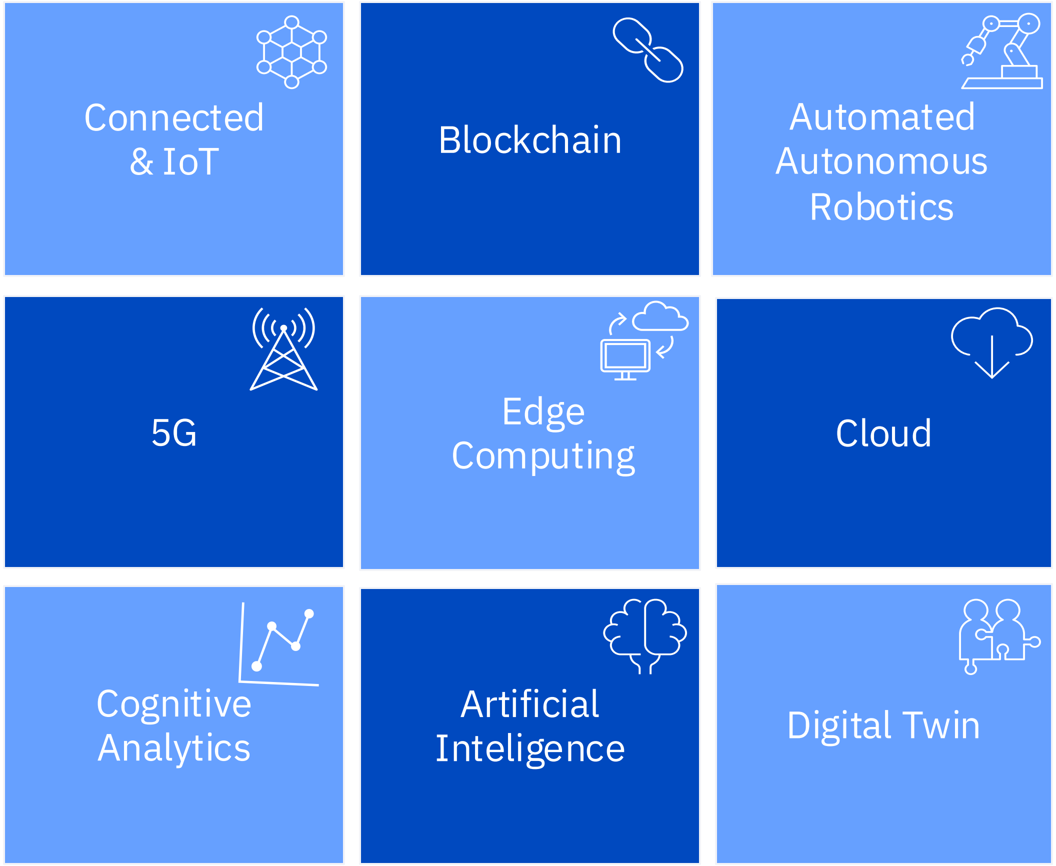
Organizations need to design and manage their privacy governance frameworks, data management systems in a global environment where the privacy challenges are multifold due to the different privacy cultures legislations.

#6 Processor Third Party Management

Organizations upon managing their privacy activities need to supervise, coordinate, manage a growing network of processors and third parties (contractors and consultants) that work together to provide products and services to the individuals.

Privacy Challenges in Digital Transformation

IBM is one of the key stakeholder in driving the digital revolution.



Connected & IoT

Blockchain

Automated Autonomous Robotics

5G

Edge Computing

Cloud

Cognitive Analytics

Artificial Inteligence

Digital Twin

<58%

Strategic Importance

“58 percent of 1,100 executives surveyed in the Digital Reinvention Study expect new technologies to reduce barriers to entry and 69 percent expect more cross-industry competition.”

Source: IBM IBV – Digital Reinvention

- ➢ Evolve
- ➢ Adapt
- ➢ Adopt

Companies are transforming their business operations due to the new and disruptive technologies, so shall they adapt their data protection frameworks to the new challenges!

Privacy data management is an iterative and continuous process

Data management is governed by laws and regulations globally, and specifically in Indonesia where organizations must comply with every aspect seen from various views of Policies, Procedures, and Controls.

Information Asset
Early identification of sensitive data/information

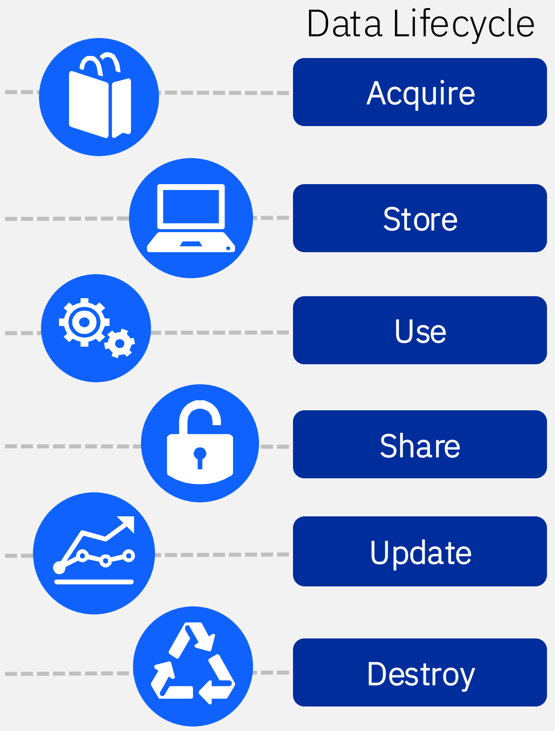
Data at Rest
Store sensitive information safely

Data in Use
Sensitive data protection is used properly

Data in Motion
Ensuring shared sensitive data is protected

Data at Rest
Provides a secure means of updating data

Data at Rest
Ensuring that data and its storage are destroyed safely



Data Lifecycle

What data is collected and "created", from whom, how is it obtained, and through what channels?

Where is the data stored - both inside and outside the company, in what systems, and in which manual repositories?

How is data used, who uses it, and what is it used for?

Who is the information shared with - inside and outside the company and across jurisdictions, why is it being shared?

How is data stored - either by the company or by third parties, for how long, and how is it destroyed?

GR No.71/2019	MR MOCI No. 5/2020	MR MOCI No.20/2016	PBI No. 22/2020	EU GDPR	PDP Bill
Article 14	Article 30,40	Article 7-10	Article 30-34, 40,42	Article 5-6, 13-15	Article 17, 19,24
Article 14	Article 30,40	Article 11,15-20	Article 30-34, 40,42	Article 5,32	Article 17,27
Article 14	Article 30,40	Article 12-14,21	Article 30-34, 40,42	Article 5, 18	Article 17,26
Article 14	Article 30,40	Article 22-24	Article 30-34, 40,42	Article 16,20	Article 34,47
Article 14-18	Article 30,40	Article 25	Article 30-34, 40,42	Article 16-17	Article 34, 37,38,39

1. Who are the executive personas

Understand the different perspectives!

CISO

Chief Information Security Officer: a policeman for protecting the integrity, confidentiality and availability of all of the enterprise data, IBM's sweet spot.

- Narrowly focused on Data Protection activities
- Looks for a way to ”check the box” for specific regulatory obligations and be done with them

CIO

Chief Information Officer: responsible for enterprise IT, IBM's sweet spot.

- Usually annoyed by added regulatory burden
- Looks for a way to ”check the box” for specific regulatory obligations and be done with them
- Oversee the implementation of data privacy in the company's IT ecosystem

CPO

Chief Privacy Officer: responsible for overall Privacy governance activities and other compliance obligations.

- Usually has a legal, enterprise-wide perspective
- Typically, he/she is overwhelmed in the role
- *How IBM can help:* provide governance assistance, assessments, corporate roadmaps

DPO

Data Protection Officer: responsible for Privacy governance activities usually with regard to a single regulation like GDPR. Sometimes is the same or reports to the CPO.

- Usually has a legal, enterprise-wide perspective but focused on one regulation
- Typically is overwhelmed in the role
- *How IBM can help:* provide governance assistance, assessments, corporate roadmaps

2. Who are the field personas

Understand the different perspectives!

IT Security

IT Security: design and implement security of IT systems

- Design and implementation of the security policy, AAA, consent management, encryption
- Create a privacy policy
- Handling privacy incidents
- Status report

Data Management

Data Management: responsible for data management and protection.

- Make documentation of personal data used
- Protect data by creating access control and authority over data
- Encryption of data at rest
- RBAC for data

Application Team

Application team: responsible for design and development of secure applications

- Implement consent and terms at application
- Ensure proper security of personal data at application layer
- Document application architecture

Process and Audit

Process and audit: Design business process and rules to comply with PDP law. Conduct internal audit for compliance.

- Update business process and rules to align with PDP law
- Audit the internal stakeholders for compliance to the process and rules
- Provide report to data processor

What capabilities should enterprises prepare?

Govern the lifecycle of personal data management

Discover personal data in the data ecosystem

Mapping data processing activities to personal data use

Consent management system and implementation on applications

Access control and authorization of data – SSO, TWA

Data at rest / in transit protection and confidentiality

Accountable personal data storage and processing

Secure infrastructure for personal data

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 III

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 IV

Data Subject Rights

Erasure, Disposal and Retention

Mandatory Elements:

- Customer Contact Point
- Request Ticketing Platform

Chapter V

Consent Management

Mandatory Elements:

- Consent Management Platform

Chapter V

Chapter VI

Policies and Procedures

Record of Processing Activity

Access Control

Data Breach Management

Data Encryption & Masking

Third Party Risk Assessment

Legitimate Interest Assessment

Data Protection Impact Assessment

Independent Department

Terminologies

Data Controller	Data Processor	Data Privacy Officer
Determining the purpose of data processing and performing control over data processing activities.	Processing personal data on behalf of the Data Controller..	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

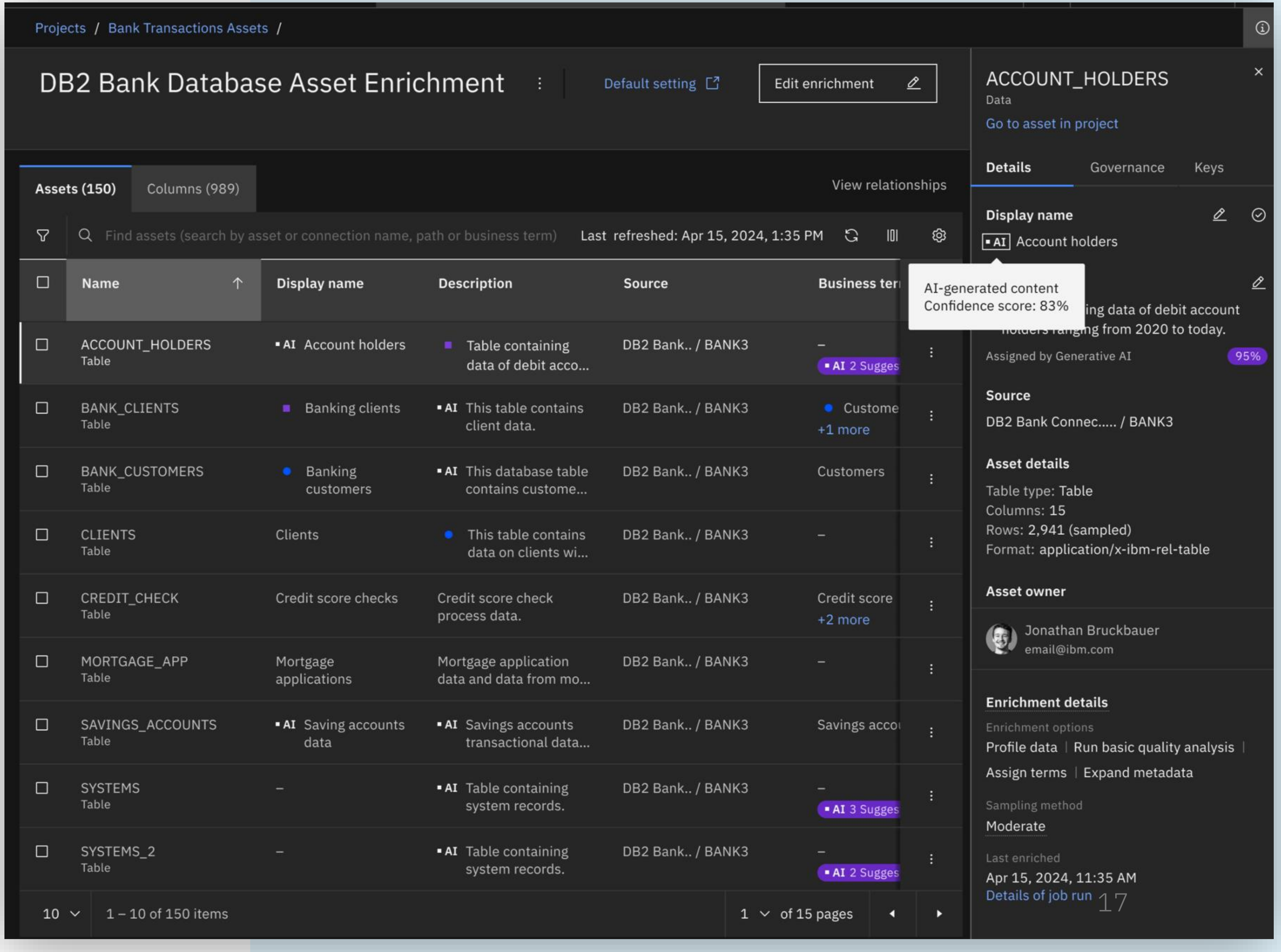
Legal, Compliance, Audit and Risk Management

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

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%

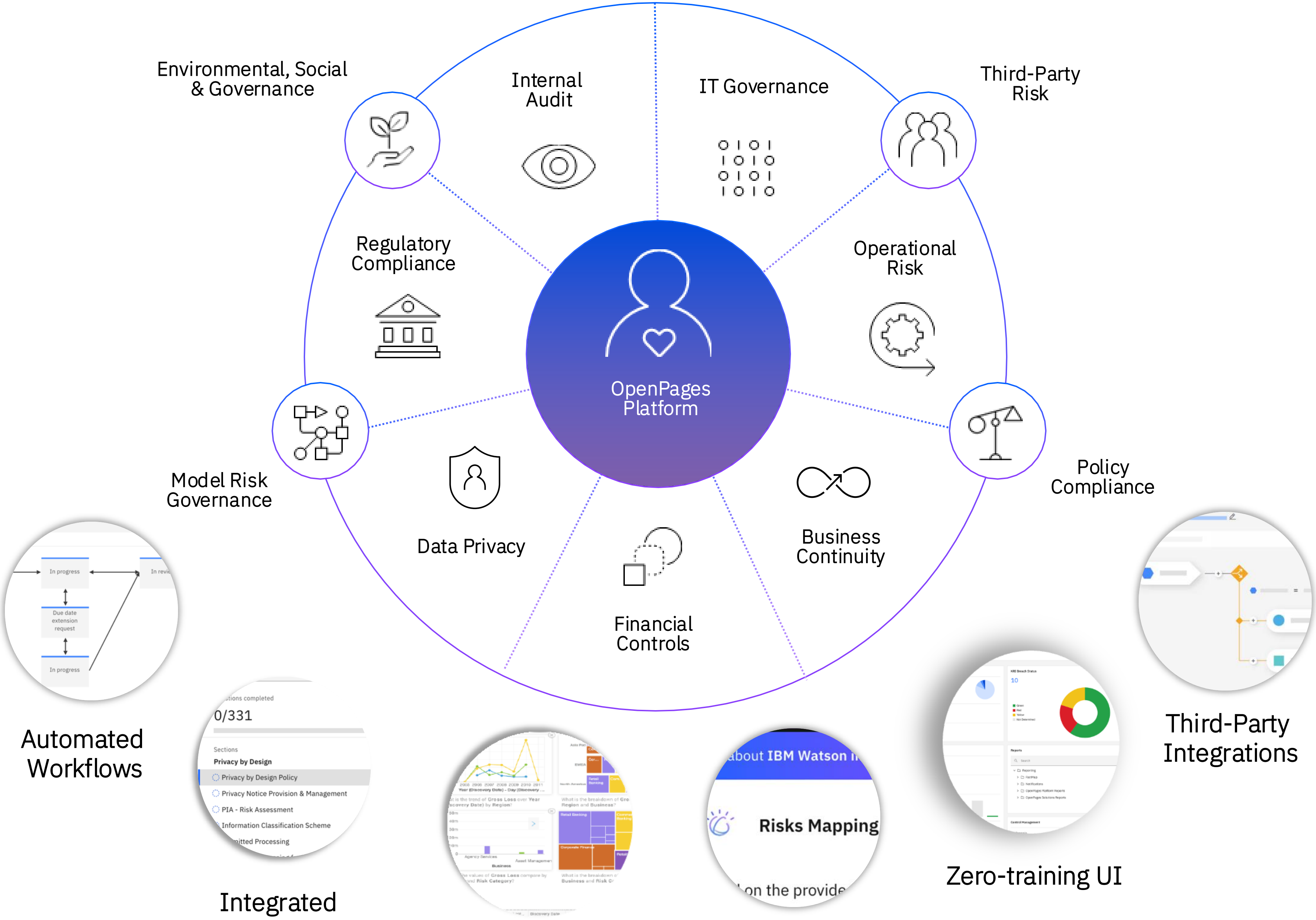
Source
DB2 Bank Connec..... / BANK3

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



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

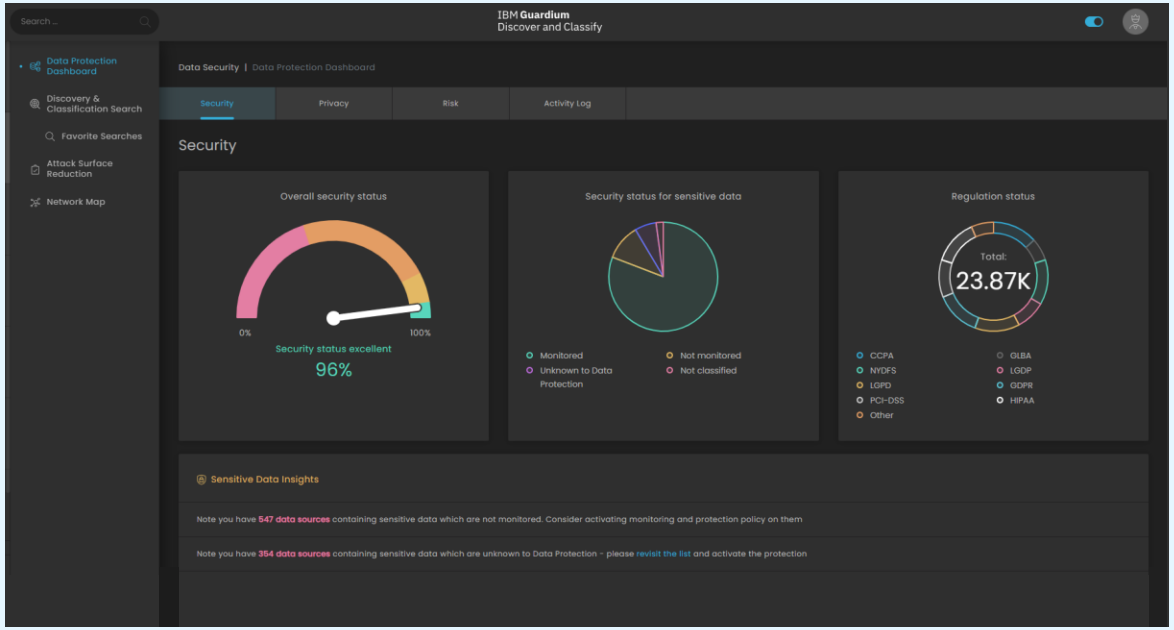
Enrich existing security and compliance tools with deep data-level context to enable smarter protection and better prioritization of defenses

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

IBM