



Navigating Compliance, The Digital Personal Data Protection Act 2023



AGENDA

- 1 Introduction
- 2 Definition
- 3 Overview of the Act
- 4 Applicability & Key Components of DPDP Act
- 5 Journey of Privacy Law in India
- 6 Personal Data Breaches Happening Around The World
- 7 Penalties for Non- Compliance
- 8 Data Protection Compliance Approach
- 9 Opportunities for CA



INTRODUCTION

- ❑ In the digital age, data has become a currency of immense value.
- ❑ India, with its rapidly growing digital landscape, is no exception to the global data revolution.

The significance of data privacy in India is underscored by several critical factors



Protecting Personal Information

01

Data privacy is fundamentally about **safeguarding personal information**. In our interconnected world, personal data is constantly being shared, collected, and analyzed. Ensuring that this data remains private and secure is paramount.



Digital Transformation

02

India's rapid digital transformation has led to the proliferation of data across sectors, from e-commerce and healthcare to education and finance. This **digitization presents both opportunities and challenges**, making data privacy a central concern.



Regulatory Framework

03

The introduction of the Digital Personal Data Protection Act (DPDPA) signifies the government's recognition of the need for comprehensive data protection laws. **Compliance with the DPDPA is not just a legal requirement** but a crucial aspect of responsible business operations



Building Trust

04

Trust is the foundation of any successful business or institution. When organizations prioritize data privacy, they demonstrate their **commitment to protecting their customers' and stakeholders' sensitive information**, ultimately building trust



Mitigating Risks

05

Data breaches and cyberattacks are on the rise globally. India is not immune to these threats. Effective data privacy measures help **mitigate the risks associated with data breaches**, safeguarding both individuals and organizations

CHALLENGES FACED BY ORGANIZATION

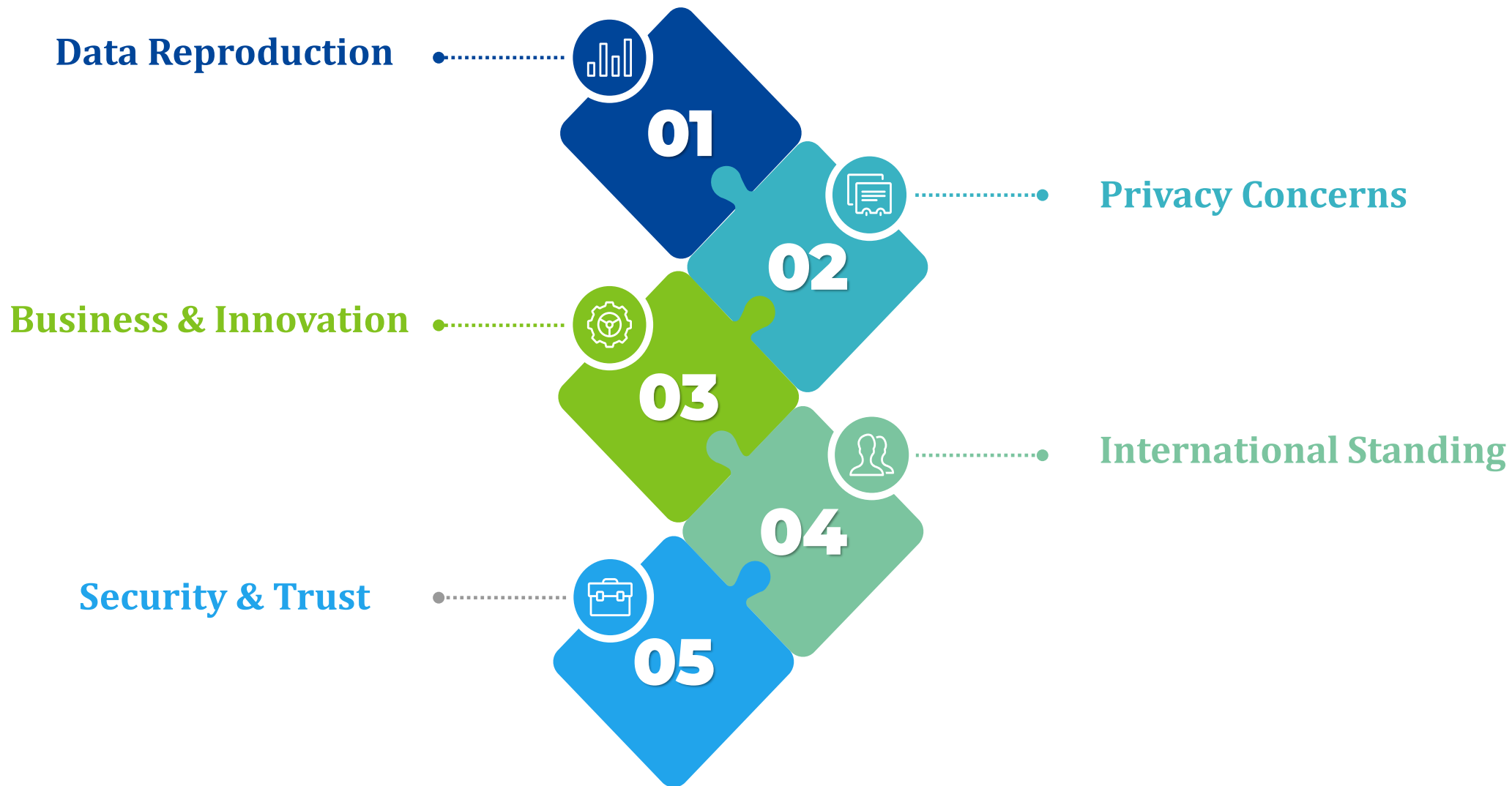


Rapid digitization and the exponential growth of data create opportunities for **cyberattacks** and **data breaches**

Cross-border data transfers and compliance with international regulations pose challenges for businesses operating globally.

Balancing innovation with data protection is a constant challenge for organizations.

NEED FOR COMPREHENSIVE DATA PROTECTION LAW IN INDIA



DEFINITION



DEFINITION

Organizations should seek a consent, which is freely given, specific, informed and unambiguous indication of the Data Principal's wishes, by a clear affirmative action

Data is a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means

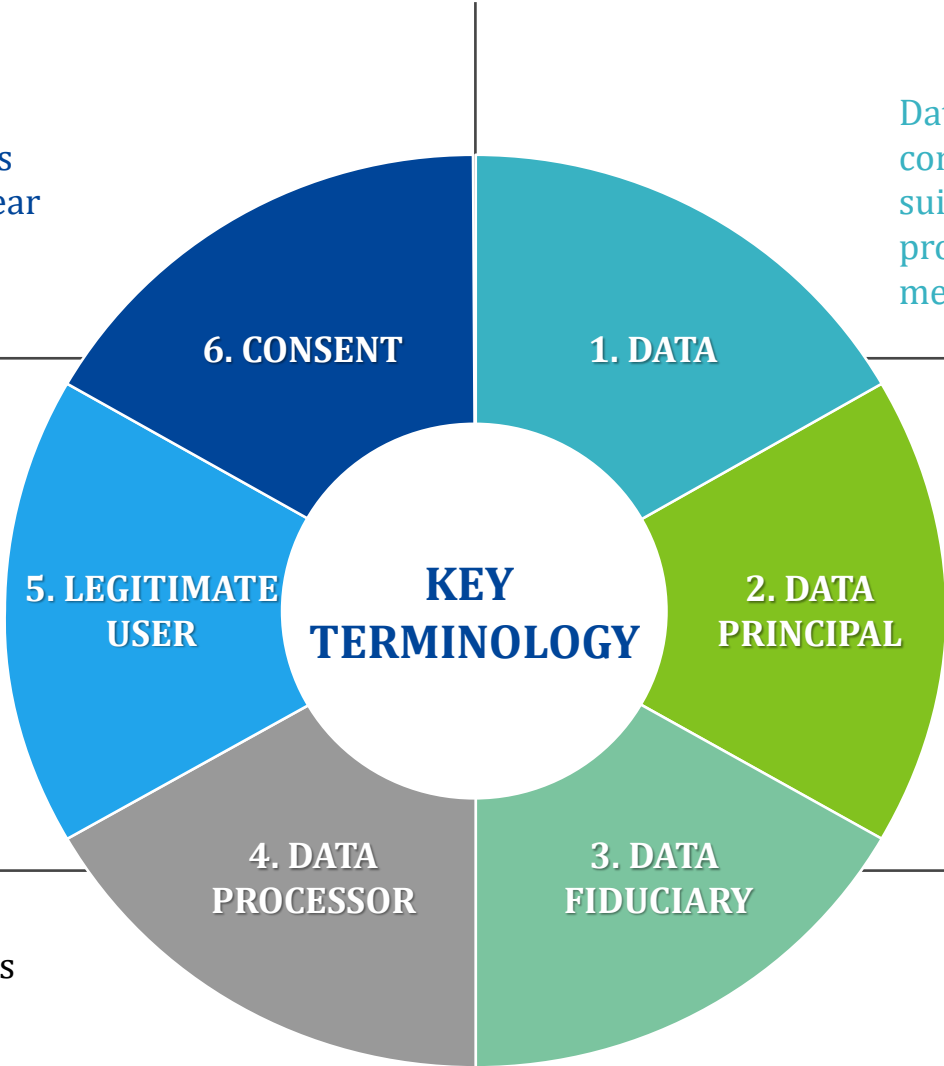
Consent is not expressly needed for situations such as

- Voluntary disclosure by data principal
- Reasonable expectation by data principal
- Performance of function under the law
- Medical emergency among others
- Compliance with any judgment issued under any law
- Threat to public health
- Ensure safety in case of any disaster

Data Processor means any person who processes personal data on behalf of a data fiduciary

- An individual to whom the personal data relates
- A child, includes the parents or lawful guardian of such a child
- A person with disability, includes their lawful guardian acting on their behalf

Data fiduciaries' as entities determining the purpose and means of processing of personal data



Personal Data

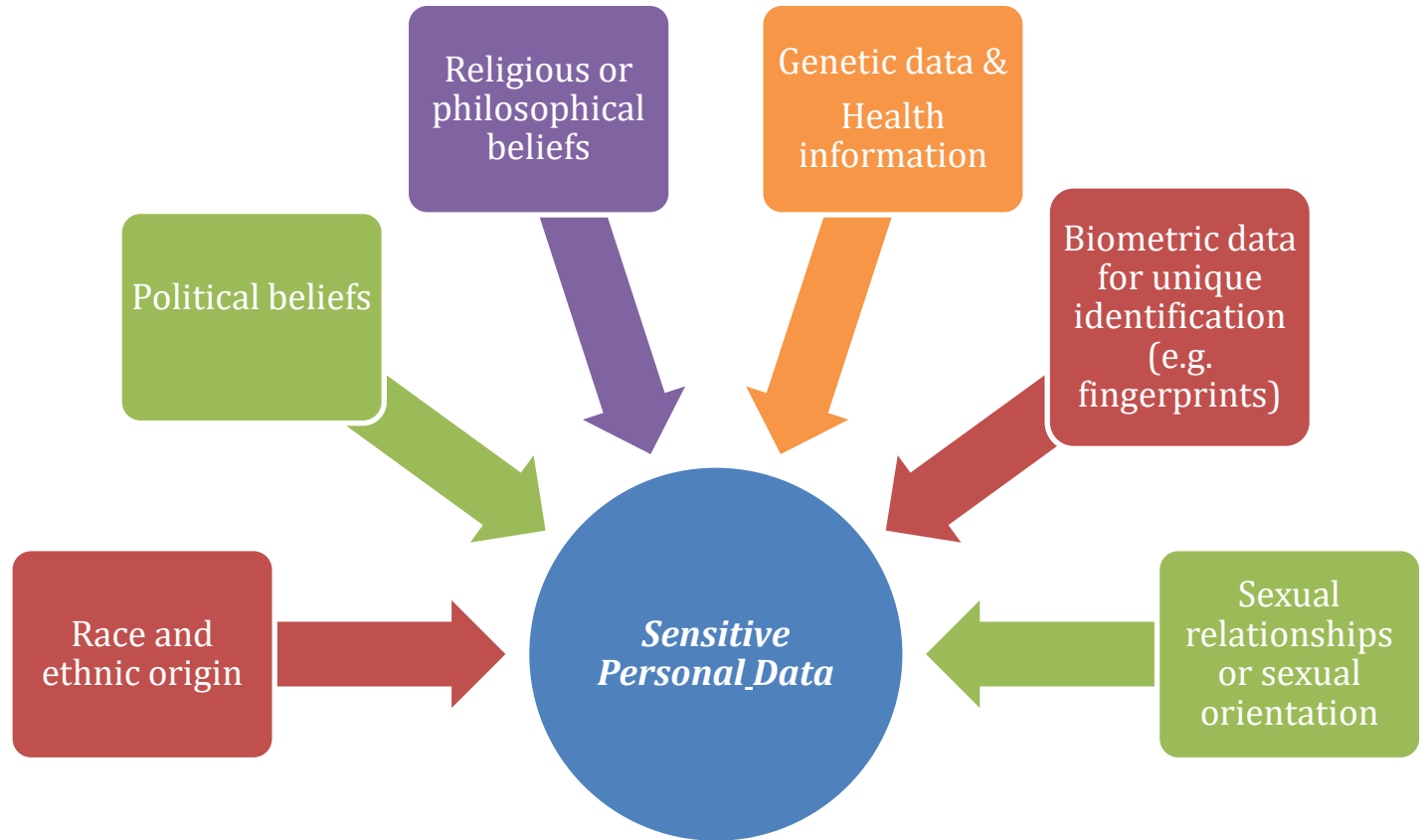
Non-Sensitive Data

Sensitive Data

Non- Sensitive Data

Employee	Non- Employee
Name	Client, Supplier & Contractors - Name, address, Contact details, ID card
Surname	
Residential Address	
Telephone Number	
ID card	
Bank Account Number	

Sensitive Data





OVERVIEW OF THE ACT

OVERVIEW OF THE ACT

PURPOSE OF THE DIGITAL PERSONAL DATA PROTECTION ACT

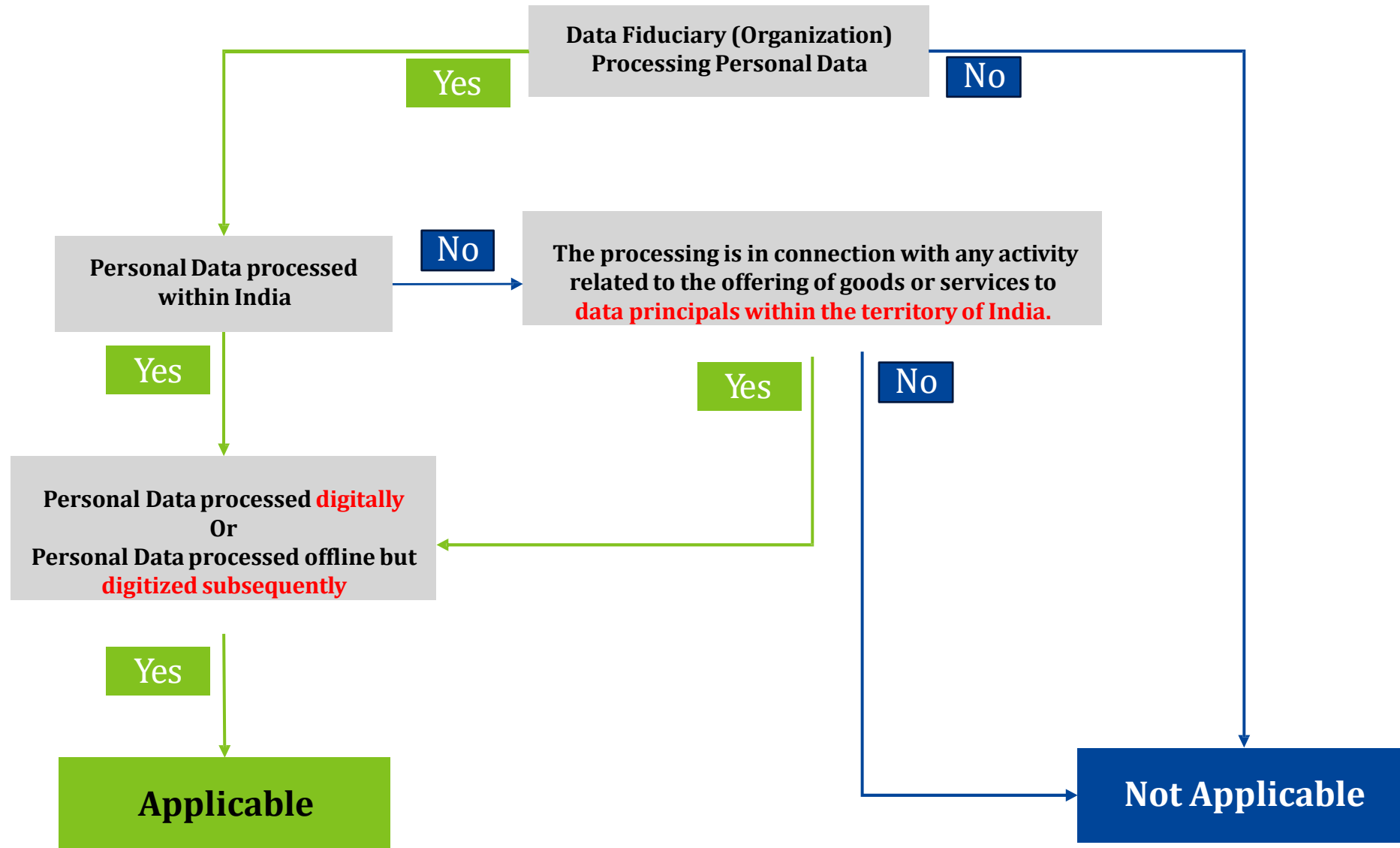




APPLICABILITY & KEY COMPONENTS OF DPDPA ACT



SCOPE & APPLICABILITY OF DPDP ACT



KEY COMPLIANCE REQUIREMENTS

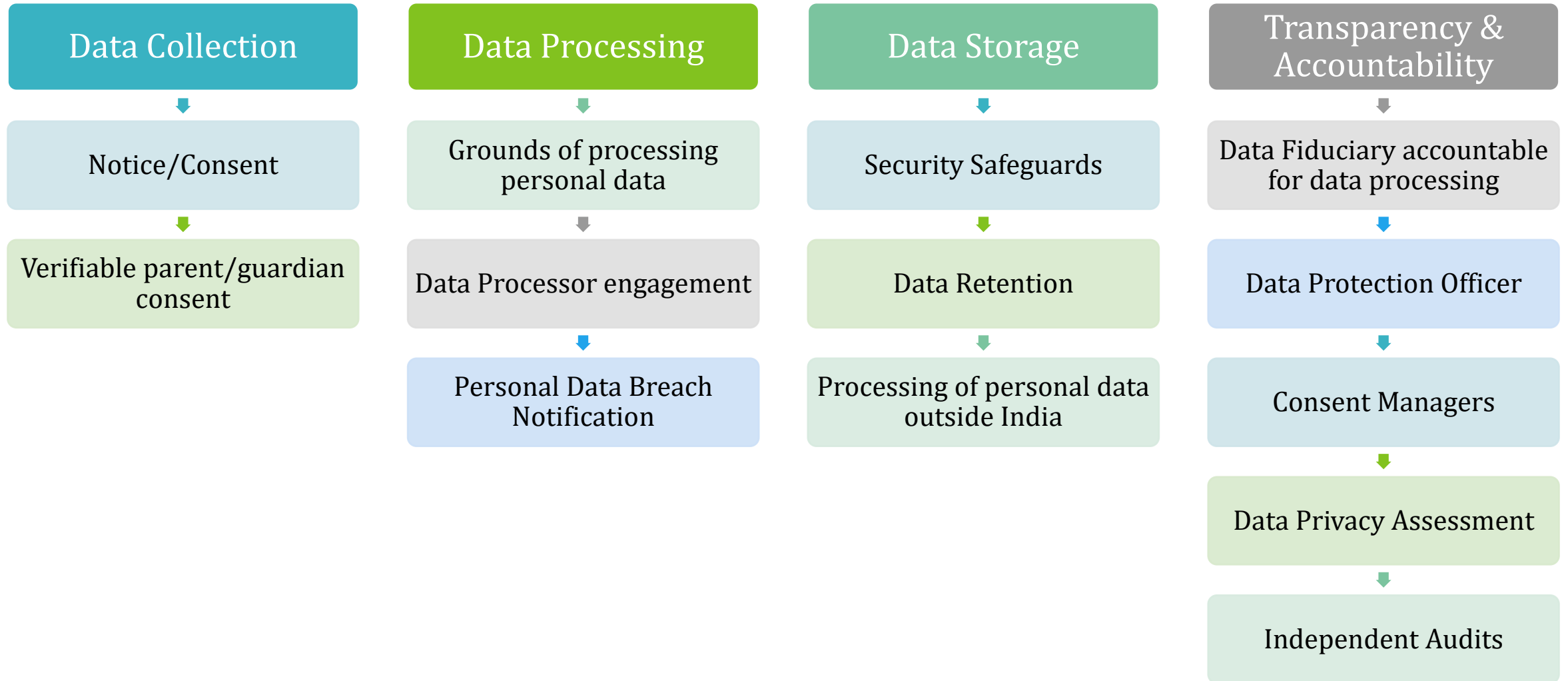


**OBLIGATION OF DATA
FIDUCIARY**



**RIGHTS OF THE DATA
PRINCIPAL**

OBLIGATION OF DATA FIDUCIARY



RIGHTS OF THE DATA PRINCIPAL

Data Collection



Consent & Consent
Withdrawals

Data Processing



Right to access information
about personal data



Right to correction of
personal data

Data Storage



Right to erasure

Transparency &
Accountability

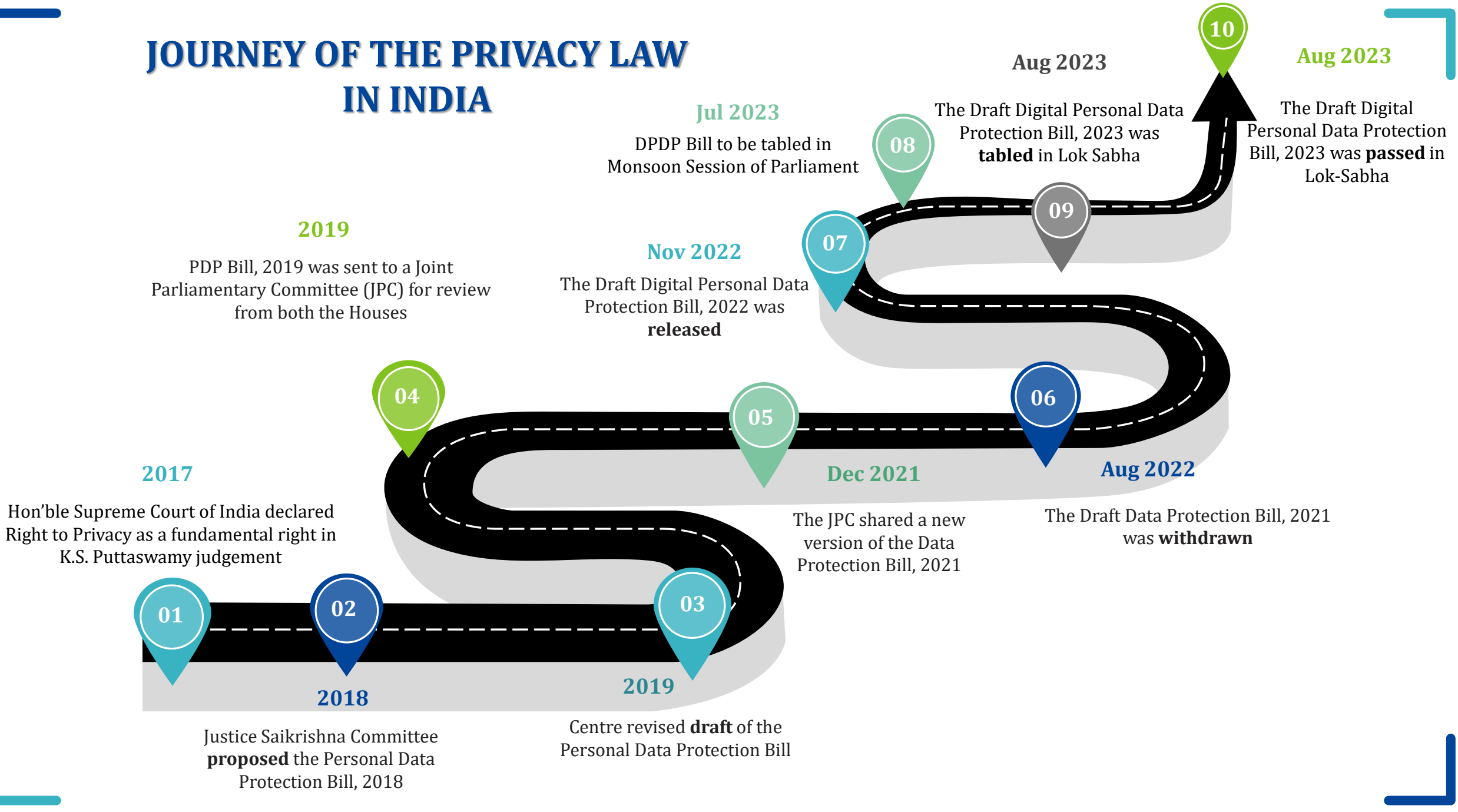


Right to grievance redressal
and nominate

An aerial photograph of a dense urban skyline, likely in South America, featuring numerous high-rise apartment buildings. The sky is dramatic, with dark, heavy clouds on the left side that transition into a bright, hazy orange and yellow light on the right side, suggesting a sunset or sunrise. The overall color palette is dominated by these warm tones and the grey of the buildings.

JOURNEY OF THE PRIVACY LAW IN INDIA

JOURNEY OF THE PRIVACY LAW IN INDIA



2017

Hon'ble Supreme Court of India declared Right to Privacy as a fundamental right in K.S. Puttaswamy judgement

01

02

2018

Justice Saikrishna Committee **proposed** the Personal Data Protection Bill, 2018

03

2019

Centre revised **draft** of the Personal Data Protection Bill

04

2019

PDP Bill, 2019 was sent to a Joint Parliamentary Committee (JPC) for review from both the Houses

05

Dec 2021

The JPC shared a new version of the Data Protection Bill, 2021

06

Aug 2022

The Draft Data Protection Bill, 2021 was **withdrawn**

07

Nov 2022

The Draft Digital Personal Data Protection Bill, 2022 was **released**

08

Jul 2023

DPDP Bill to be tabled in Monsoon Session of Parliament

09

Aug 2023

The Draft Digital Personal Data Protection Bill, 2023 was **tabled** in Lok Sabha

10

Aug 2023

The Draft Digital Personal Data Protection Bill, 2023 was **passed** in Lok-Sabha

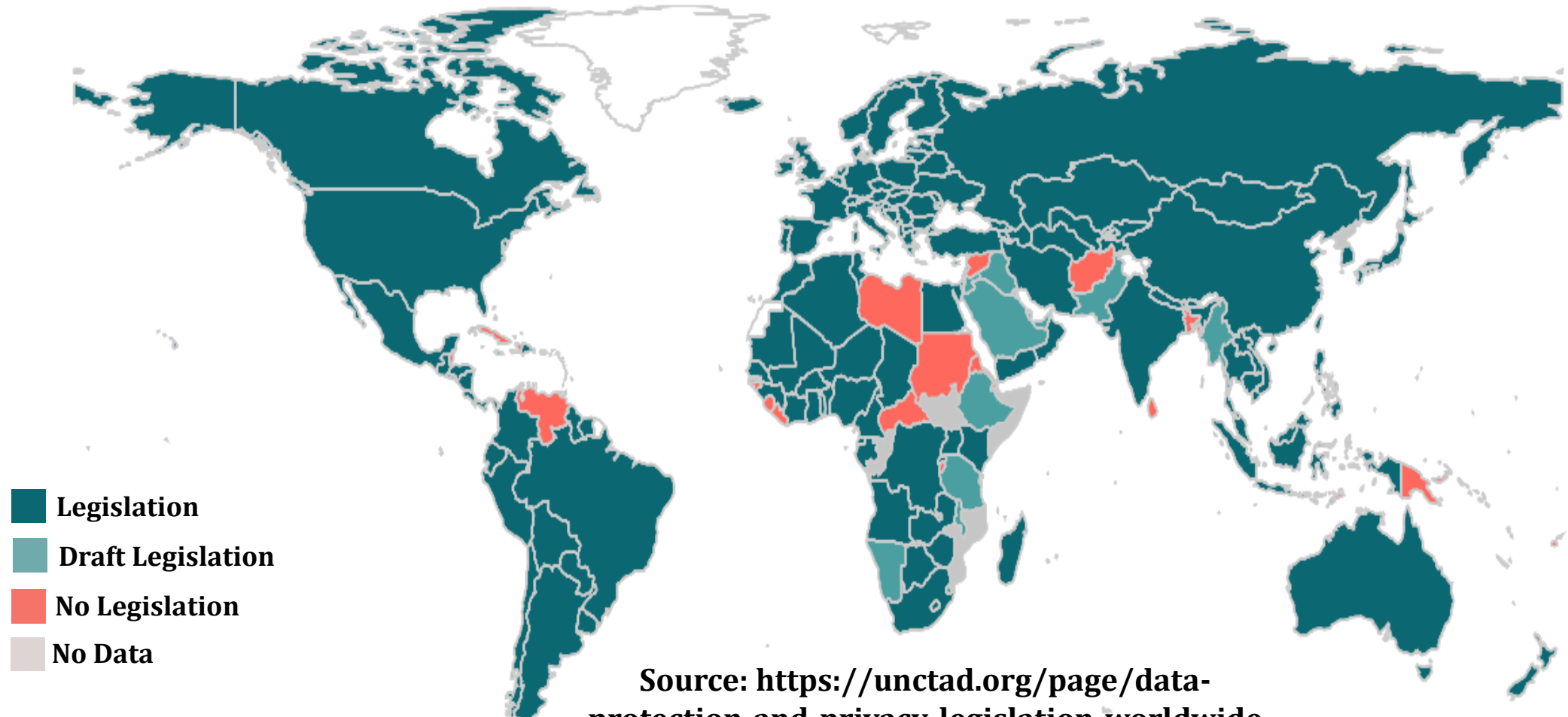
DATA PROTECTION AND PRIVACY LEGISLATION WORLDWIDE

71 %
COUNTRIES WITH
LEGISLATION

9 %
COUNTRIES WITH
DRAFT LEGISLATION

15 %
COUNTRIES WITH
NO LEGISLATION

5 %
COUNTRIES WITH
NO DATA



Source: <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>

The background features a collage of newspaper clippings with various headlines related to data breaches. Visible headlines include 'BUSINESS NEWS', 'DATA STOLEN', 'FEKL...', 'DATA BREACH', 'FINANCIAL NEWS', 'DATA BREACH', 'NEWS TODAY', and 'HACKED!'. The clippings also contain some graphical elements like bar charts and pie charts. Overlaid on this collage is a dark silhouette of a person sitting at a desk, leaning forward with their hand to their chin in a thoughtful or concerned pose. The overall color palette is muted, with shades of brown, tan, and grey.

**PERSONAL DATA BREACHES HAPPENING
AROUND THE WORLD**

BIGGEST DATA BREACHS

Meta

- **€1.2 billion (\$1.3 billion)**
- Data shipped across the Atlantic was not sufficiently protected from American spy agencies.

Amazon

- **€746 million (\$781 million)**
- Amazon was not getting consent from its users before storing advertisement cookies.

Instagram

- **€405 million (\$427 million)**
- The EU regulator found that Instagram operated a user registration system which could lead to the accounts of child users being set to “public” by default, unless changed to “private.”
- This went against the privacy by design guidelines of the GDPR as well as provisions aimed at enhancing the protection of children’s information

TikTok

- **€345 million (\$377 million)**
- Users aged between 13 and 17 were steered through the sign-up process in a way that resulted in their accounts being set to public – meaning anyone can see an account’s content or comment on it.

BIGGEST DATA BREACHS

Facebook

- **€265 million (\$275 million)**
- The data was found on a website for hackers and included names, Facebook IDs, phone numbers, locations, birthdates, and email addresses of people from more than 100 countries.

WhatsApp

- **€225 million (\$247 million)**
- Regulators eventually decided that the company had not been transparent enough about the mechanisms it uses to store and share data

Google LLC

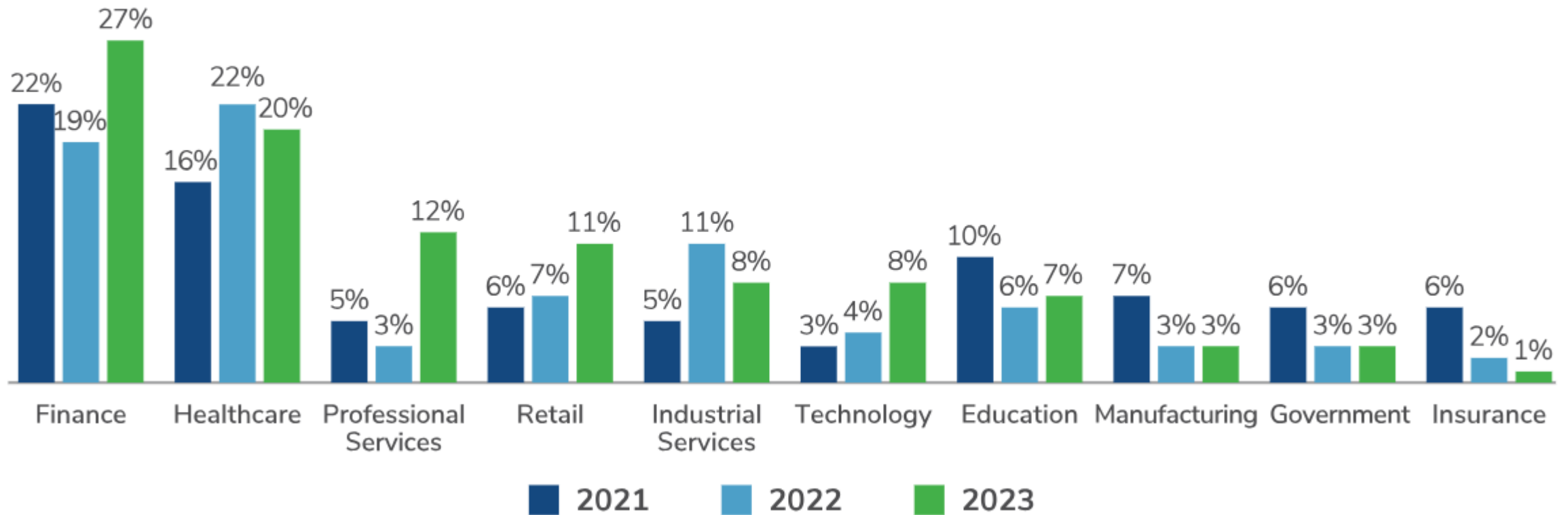
- **€150 million (\$169 million)**
- Noncompliant cookie consent mechanisms, making it difficult for users to refuse cookies on Google and YouTube.

H&M

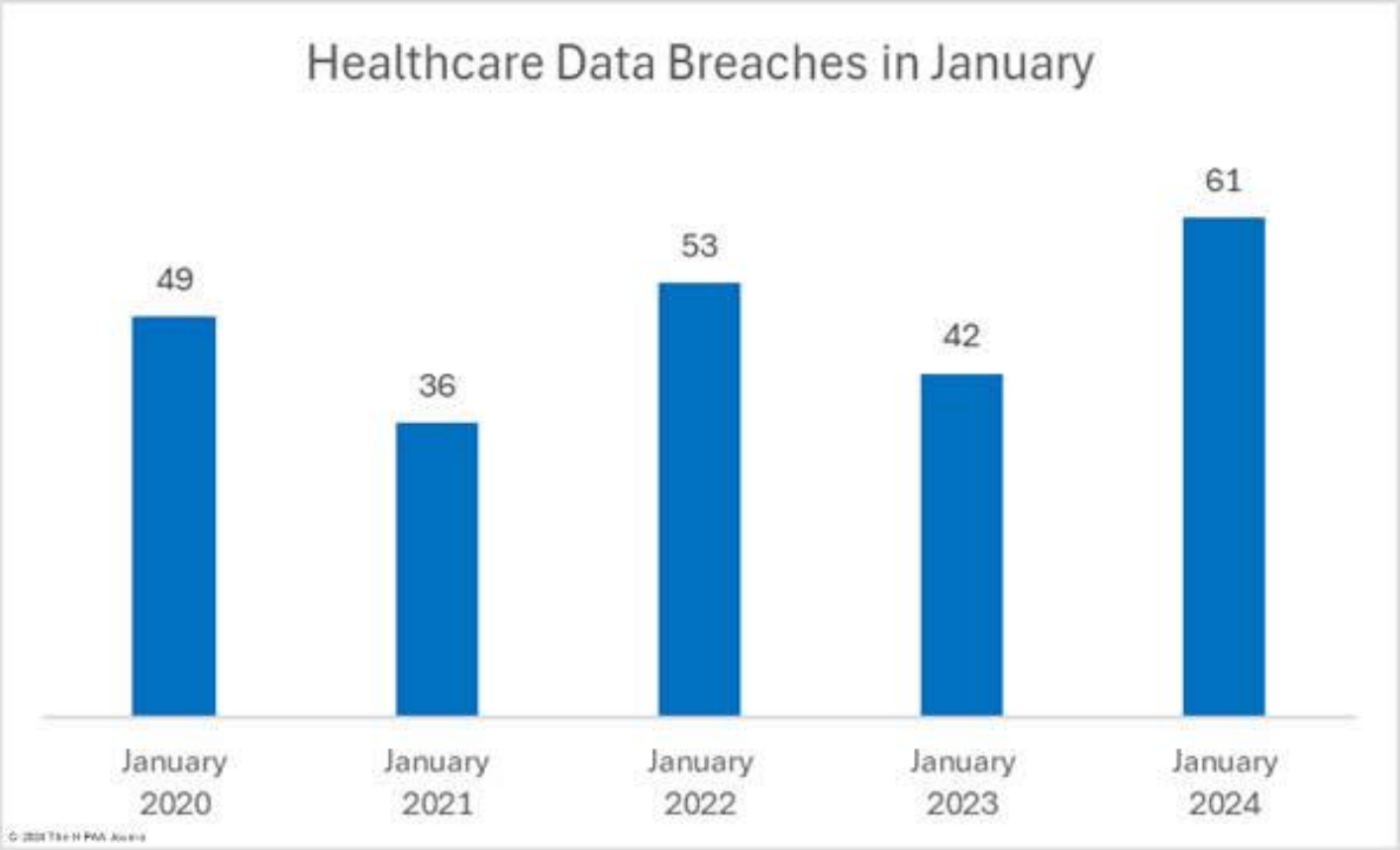
- **€35 million (\$41 million)**
- The company kept "excessive" records on the families, religions and illnesses of its workforce details of holidays, medical symptoms and diagnoses for illnesses. Which were then used to evaluate work performance and make employment decisions

DATA BREACH STATISTICS 2021 to 2023

Percentage of Data Breaches a From 2021 to 2023, by Industry



HEALTH CARE DATA BREACH STATISTICS 2020 to 2024



Source: <https://www.hipaajournal.com/january-2024-healthcare-data-breach-report/>



PENALTIES FOR NON- COMPLIANCE

S. No.	Breach Description	Penalty
1	Breach in observing the obligation of Data Fiduciary to take reasonable security safeguards to prevent personal data breach	Up to 250 crore rupees
2	Breach in observing the obligation to give the Board or affected Data Principal notice of a personal data breach	Up to 200 crore rupees
3	Breach in observance of additional obligations in relation to children	Up to 200 crore rupees
4	Breach in observance of additional obligations of Significant Data Fiduciary	Up to 150 crore rupees
5	Breach in observance of the duties	Up to 10,000 rupees
6	Breach of voluntary undertaking accepted by the Board	Up to the extent applicable to the breach under section 28
7	Breach of any other provision of this Act or rules	Up to 50 crore rupees



DATA PROTECTION COMPLIANCE APPROACH

DATA PROTECTION COMPLIANCE APPROACH

**Data Discovery &
Data Classification**

1

**Data Protection
Impact Assessment**

2

**Privacy Risk
Assessment**

3

**Technical and Policy remediation
roadmap and support**

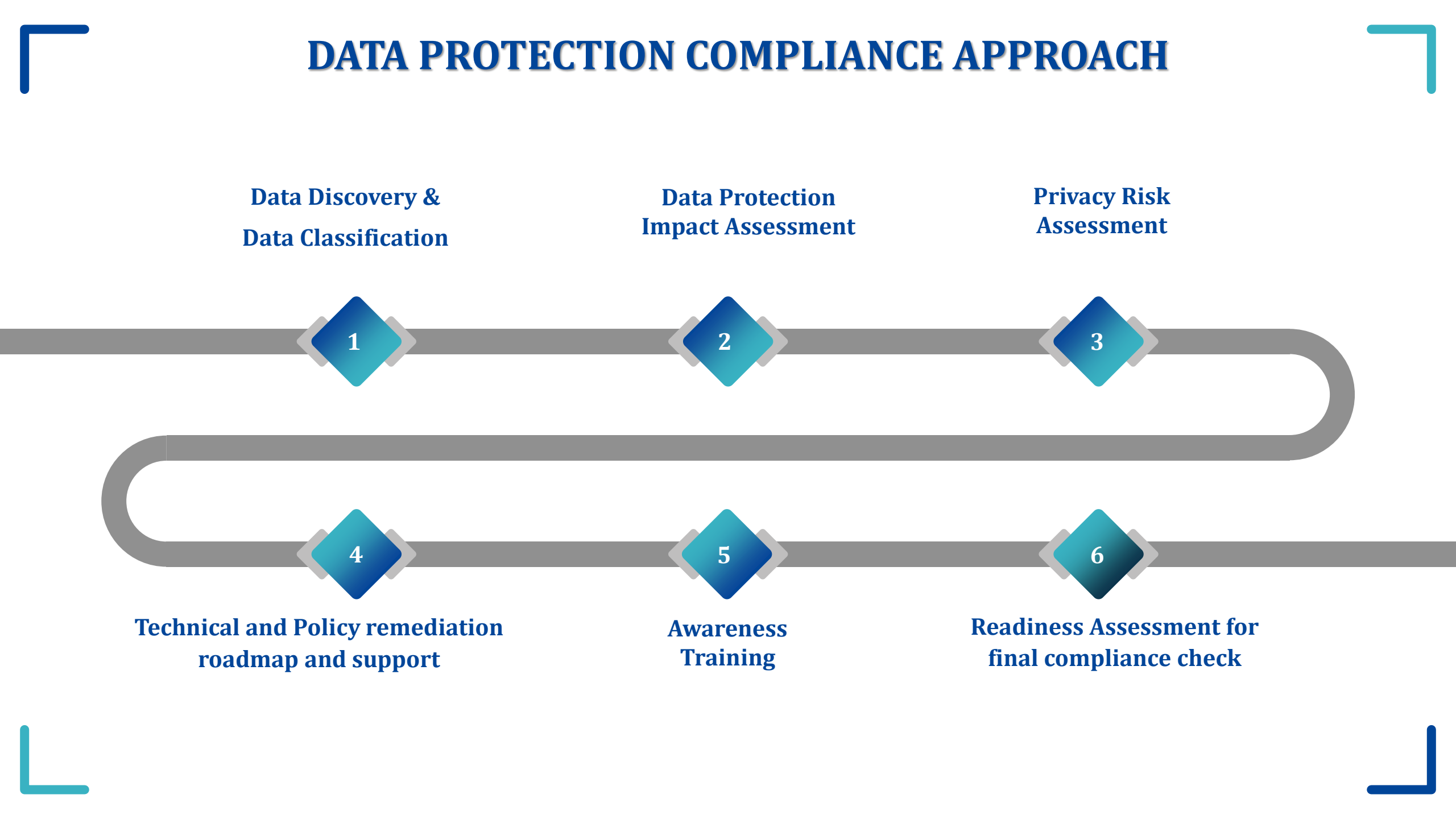
4

**Awareness
Training**

5

**Readiness Assessment for
final compliance check**

6



DATA DISCOVERY & CLASSIFICATION

Data Discovery



- Identify Data
- Locate Personal Data
- Stored, Processed & Transmitted

Data Classification



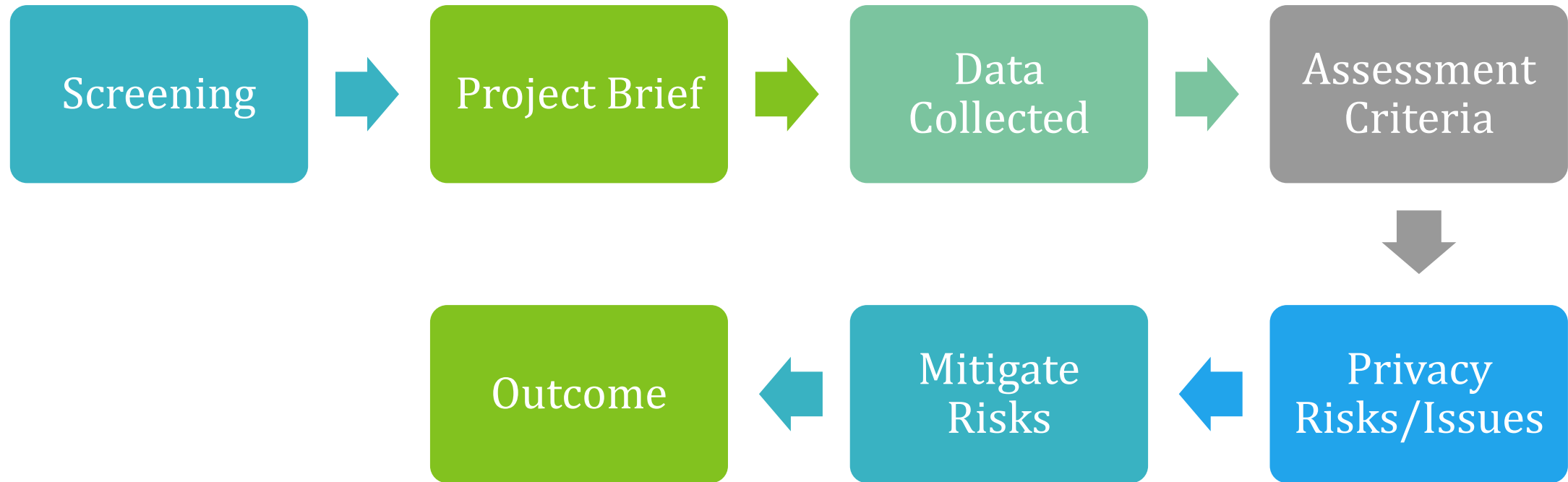
- Classify Data based on sensitivity
- Personal Data
- Sensitive Personal Data

Create a data inventory and update it regularly.

DATA PROTECTION IMPACT ASSESSMENT

A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimize the data protection risks of a project.

The DPIA consists of the below sections: -



PRIVACY RISK ASSESSMENT

A privacy risk assessment is a risk management framework for determining the risk of holding and maintaining PII (Personal Identifiable Information). Organizations can make informed decisions to prevent privacy-related risk by conducting privacy risk assessments. Analyze if controls are in place to identify and reduce privacy risk, focusing on compliance with privacy regulations



PIA vs DPIA

Aspect	Privacy Impact Assessment	Data Protection Impact Assessment
Purpose	Analyze if controls are in place to identify and reduce privacy risk , focusing on compliance with privacy regulations.	Assess and mitigate high risks to data Principal rights and freedoms arising from data processing activities.
Scope	Covers a broad range of data processing activities and organizational practices.	Focuses on specific data processing activities with high-risk potential.
Compliance Focus	Emphasizes organizational compliance with privacy regulations.	Prioritizes assessment of potential high risks to data Principal rights and freedoms.
Risk Analysis	Evaluates privacy risks and identifies areas of non-compliance with privacy regulations.	Concentrates on identifying and mitigating high risks to individuals' rights and freedoms.
Triggering Factors	Typically conducted for standard privacy assessments.	Required when specific criteria are met, such as high-risk processing activities like profiling or surveillance.
Examples of Scenarios	<ul style="list-style-type: none"> Assessing the privacy impact of a new marketing campaign. Ensuring compliance with data protection laws for customer data. Reviewing the privacy implications of a website's data collection practices 	<ul style="list-style-type: none"> Evaluating the risks associated with collecting biometric data from employees. Conducting a DPIA for a large-scale facial recognition system in public areas. Conducting a DPIA for automated data collection and processing systems.

Technical and Policy remediation roadmap and support

#	Policies & Procedures Documents
1	Data Protection Policy and Procedure
2	Privacy Policy
3	Pseudonymization and anonymization Guidelines
4	Data Retention _ Erasure Policy
5	DPIA Procedure
6	PII principal request handling procedure
7	Data Protection Officer Roles and Responsibilities
8	Transfers of PII to third countries and international organizations procedure
9	Legitimate Interests Assessment Procedure
10	Data Breach Policy _ Procedures
11	Privacy Policy Statement

AWARENESS TRAINING

Data privacy and data privacy awareness helps to educate to educate employees about data privacy regulations, best practices, company privacy procedures, and the importance of protecting sensitive information.

Objectives

- Educate employees on protecting sensitive information.
- Ensure understanding of legal and regulatory requirements.



READINESS ASSESSMENT FOR FINAL COMPLIANCE CHECK

Perform regular audits to ensure compliance with DPDP 2023

Regularly review and update policies & procedures

Identify & remediate any compliance gaps

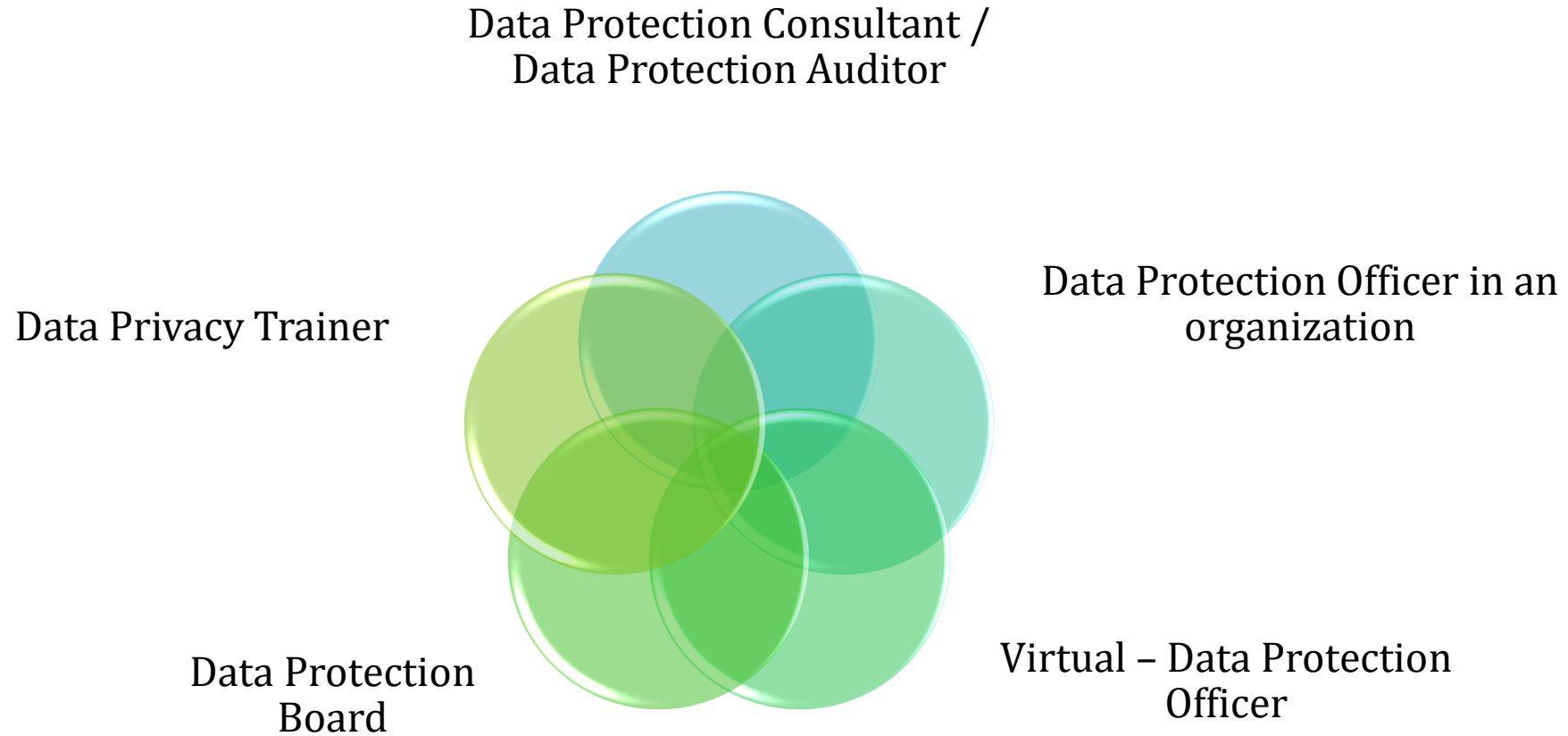
Document findings

Compliance checks and remediation action to be recorded

A man in a dark suit is seen from behind, holding a smartphone in his right hand and pointing with his left hand at a glowing point on a digital world map. The map is overlaid on a city skyline and features a network of white lines connecting various points across the globe. The text "OPPORTUNITIES FOR CA" is centered on a dark blue horizontal band across the middle of the image.

OPPORTUNITIES FOR CA


Career Opportunities in Data Protection and Privacy Laws




Questions ?

CONTACT INFORMATION

Contact

 **9940221905**
Aayush Jain

 **Email**
aayush@saaasllp.com

 **Address**
Hardevi Chambers,
Office No: 75, 2nd Floor, 103/16, Pantheon Road,
Egmore, Chennai-600008,
Tamil Nadu, India.



THANK YOU