WhitePaper

DRAFT PERSONAL DATA PROTECTION BILL, 2019

Your Guide to Compliance

INTRODUCTION

The Personal Data Protection Bill, 2019 (PDPB) was introduced in Lok Sabha on 10th December 2019. It has made significant changes from the previous Bill. The PDPB was approved by the Union Cabinet and is currently under review by the Joint Parliamentary Committee. The Bill classifies data as personal, sensitive, and critical personal data. The main authority to supervise the implementation of this law will be the Data Protection Authority (DPA). Once the Bill comes into force, organizations will have to comply with this new paradigm by establishing a robust privacy and data protection framework.

APPLICABILITY

The Bill classifies those collecting and processing data as Data Fiduciaries and Data Processors. It covers three entities:

- *the government*
- *companies incorporated in India*
- *foreign companies dealing with the personal data of individuals in India.*

DEFINITIONS

01. Data Fiduciary

Any person, including the State, a company, any juristic entity, or any individual who alone or in conjunction with others determines the purpose and means of the processing of personal data

02. Significant Data Fiduciary (SDF)

Data fiduciaries to be classified as significant data fiduciary by the Authority, based on: • volume and sensitivity of personal data processed • turnover • risk of harm resulting from any processing or any kind of processing undertaken • use of new technologies for processing.

03. Data Processor

Any person, including the State, a company, any juristic entity, or any individual, who processes personal data on behalf of a data fiduciary.

04. Data Principal

The natural person to whom the personal data relates.

KEY PROVISIONS

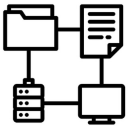
The bill departs from its draft version of 2018. These changes can be placed into three broad categories: changes to select provisions; insertions of additional obligations; and removal of certain provisions from the earlier version of the bill. Some key obligations under the PDPB will be examined in this section.

Privacy by design policy

Under Clause 22 every data fiduciary shall prepare privacy-by-design policy in accordance with the regulations which are yet to be formulated.

Privacy by design policy

A consent manager can be appointed by a data principal who will enable a data principal to withdraw, review and manage consent through a platform. Registration with the DPA is a must.



Transfer of data and localization requirement

Personal data: stored and transferred outside India
Sensitive personal data: stored in India and transferred only under specified circumstances.
Critical personal data: Processed only in India and transfer outside India only under certain exceptions.

Sandbox provisions

It is to Encourage innovation in the field of emerging technologies such as AI and machine learning, in the public interest. Data fiduciaries whose Privacy by Design policy has been certified by the authority will be eligible to apply for inclusion in the sandbox.

Transparency in processing

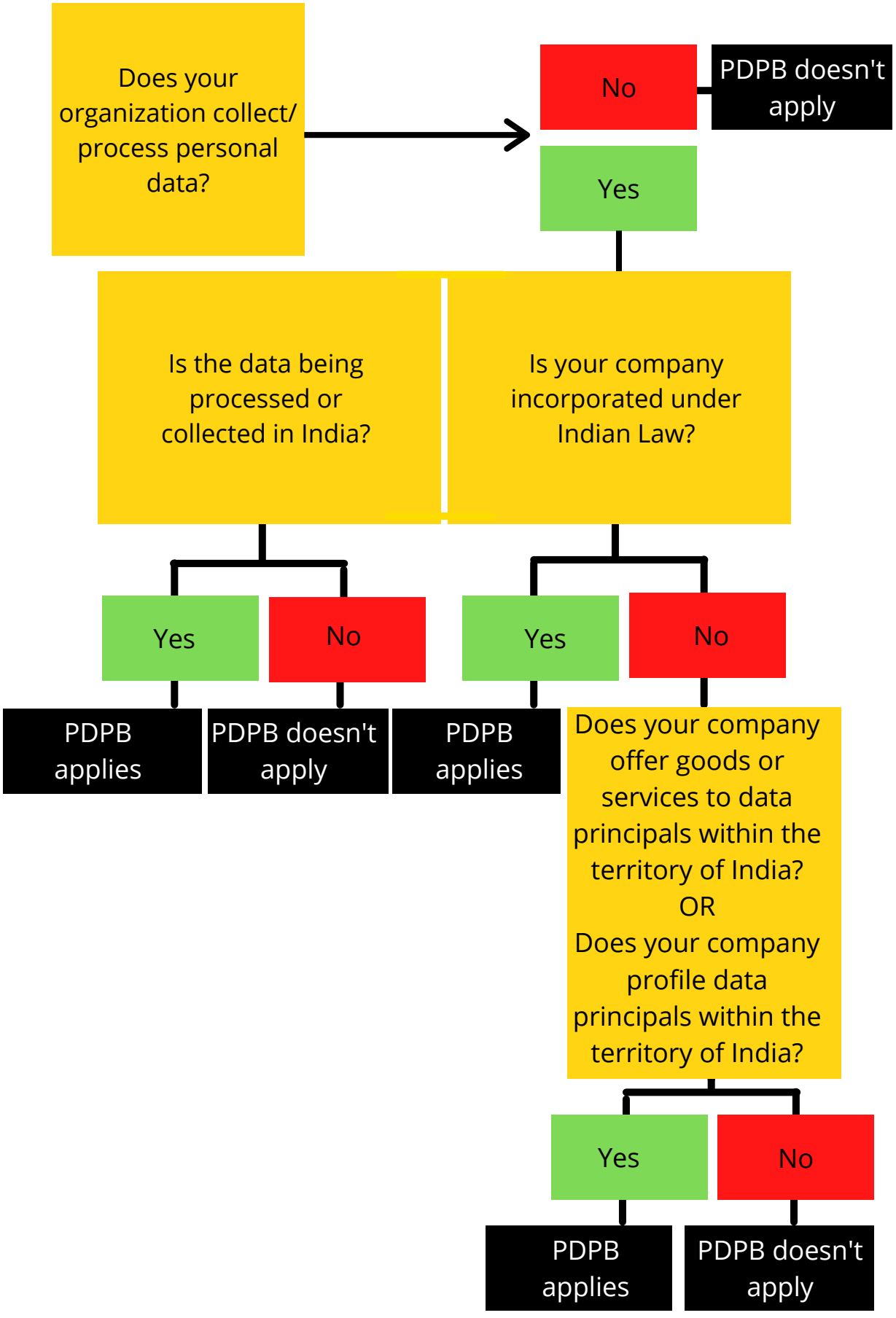
Every data fiduciary must inform the data principal on the purpose of data collection and processing and make their information available for rectification.

Data Protection Officer (DPO)

Every significant data fiduciary shall appoint a DPO whose functions are prescribed in Section 30.

APPLICABILITY CHART

This chart will help in determining whether the Draft PDPB will apply to your organization.



HOW TO ACHIEVE COMPLIANCE

The PDPB places additional obligations on Significant Data Fiduciaries as compared to Data Fiduciaries. The Bill imposes hefty fines of up to 2%- 4% of the Data Fiduciary's total worldwide turnover, in case of non-compliance.

01. Appoint a Data Protection Officer

Only for an SDF. A DPO must possess such qualifications and experience as may be specified by the regulations passed, for carrying out certain functions. The DPO is to be based in India.

02. Create a privacy by design policy

The policy must be submitted to the DPA for certification. Once certified the policy must be published on the data fiduciary's website and by the DPA.

03. Conduct Data Protection Impact Assessment

A DPIA must contain: i. A detailed description of the processing operation ii. Assessment of the potential risk that may be caused to the data principal iii. Measures to manage, mitigate, or remove such risks identified.

04. Maintain records of processing activities

Processing activities must include information about data processing, data categories, the group of data subjects, the purpose of the processing and the data recipients.

05. Register with the DPA

This is mandatory only in case of significant data fiduciaries.

06. Conduct data audit of privacy policies

The audit can be carried out by a Data Auditor.

Key Obligations	SDF	Data Fidicuciaries
Appoint a Data Protection Officer	Mandatory	Non- Mandatory
Privacy by design policy	Mandatory	Mandatory
Conduct Data Protection Impact Assessment	Mandatory	Non-Mandatory
Maintain records of processing activities	Mandatory	Mandatory
Register with the DPA	Mandatory	Non- Mandatory
Conduct data audit of privacy policies	Mandatory	Non- Mandatory

COMPANY PROFILE

Tsaaro provides privacy and cybersecurity services to help organizations meet regulatory requirements while maintaining a robust security infrastructure.

Our industry-standard privacy services include Privacy compliance, DPO-as-a-service, DPIA to name a few, delivered by our expert privacy professionals recognized by IAPP.

We take a pragmatic, risk-based approach to provide our clients with real-world, workable advice, and support, that helps them deal with a wide range of security and privacy challenges.

OUR TEAM

- **Akarsh Singh**

(CEO & Co-Founder Tsaaro)

Akarsh is a Fellow in Information Privacy by IAPP, the highest certification in the field of privacy. His expertise lies in Data Privacy and Information Security Compliance.

- **Krishna Srivastava**

(Co-Founder & Head of Cyber Tsaaro)

Krishna is an xKPMG data security consultant. He has vast experience in Information Security and Data Privacy Compliance.

REVIEWERS

- **Anoop S**

(Product Evangelist at OneTrust)

Anoop works with OneTrust in helping organizations operationalizing their privacy and security requirements

- **Lathamani BR**

(Privacy Specialist at Intel Corporation)

Latha has approximately 14 years of experience in Data Privacy and Information Security. Her expertise lie in IT Risk Management, Network Security an Privacy assessments.

CONTACT US

You can assess risk with respect to personal data and strengthen your data security by contacting Tsaaro.

Address:

Manyata Embassy Business Park, Ground Floor, E1 Block, Beech Building, Outer Ring Road, Bangalore- 560045
P: +91-0522–3581306

Regus Schiphol Rijk Beech Avenue 54-62, Het Poortgebouw, Amsterdam, 1119 PW, Netherlands
P: +31-644837150

Email us:
info@tsaaro.com