

Deloitte.



**Privacy and
Data Protection**

Draft Personal Data
Protection Bill 2018:
A Summary

For Private Circulation Only
August, 2018

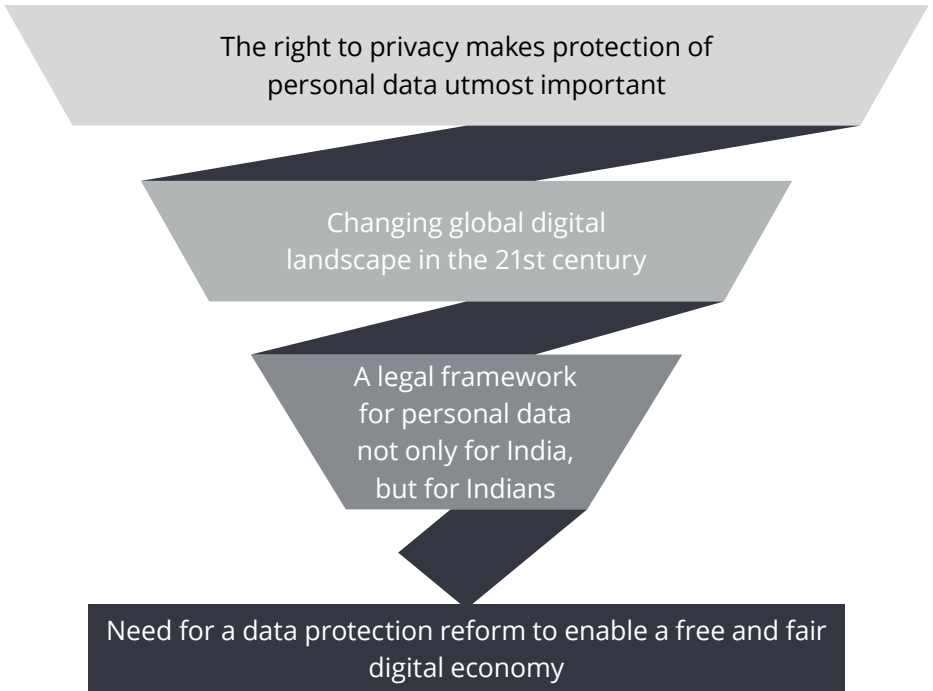
Risk Advisory ●

Introduction

Protection of personal data of data principal* is at the core of the draft Personal Data Protection Bill, 2018 (hereafter referred as “PDPB” or “bill”).

This means once the bill is enacted and enforced, privacy will no longer be optional and cannot be ignored. Among many significant provisions, the PDPB proposes substantial penalty for violation of the stated requirement.

Such provisions along with heightened focus on collection and use of personal data, will require organisations (referred in the bill as Data Fiduciary and Data Processor) to revisit their risk acceptance criteria and establish a robust privacy and data protection framework.



Understanding the construct of the bill

15
Chapters

112
Sections

4
Rights offered for
Data Principals /
Individuals

67
Pages

5
Grounds for
processing
of sensitive
personal data

11
Measures to ensure
transparency
and establish
accountability

7
Rules for
exemptions

6
Grounds for
processing of
personal data

3
Months from the notified
date for the Data Protection
Authority to be established
by the central government

Key propositions from the draft bill



Data Protection Authority of India

Bill proposes to establish an independent authority to oversee the enforcement of the provisions of the Bill.



Individual Rights

Bill proposes certain rights for data principles such as Right to access and confirmation, Right to be forgotten etc.



Territorial coverage beyond India

to organisations processing the personal data that has a connection with any business carried on in the territory of India or has any connection with any activity which involves the profiling of data principles within the territory of India



Penalties of upto to Rs. 15 Cr (~USD 2.25M) or 4% of total worldwide turnover



Data Localisation

Bill proposes that at least one serving copy of personal data is stored in India

Implications

Penalty will be imposed if the following obligations are violated:

INR 15 cr or **4%** of global turnover, whichever is higher

- 01 Prompt action in response to a data security breach
- 02 Undertaking a data protection impact assessment by a significant data fiduciary*
- 03 Conducting a data audit by a significant data fiduciary
- 04 Appointment of a data protection officer by a significant data fiduciary
- 05 Failure to register with the Authority

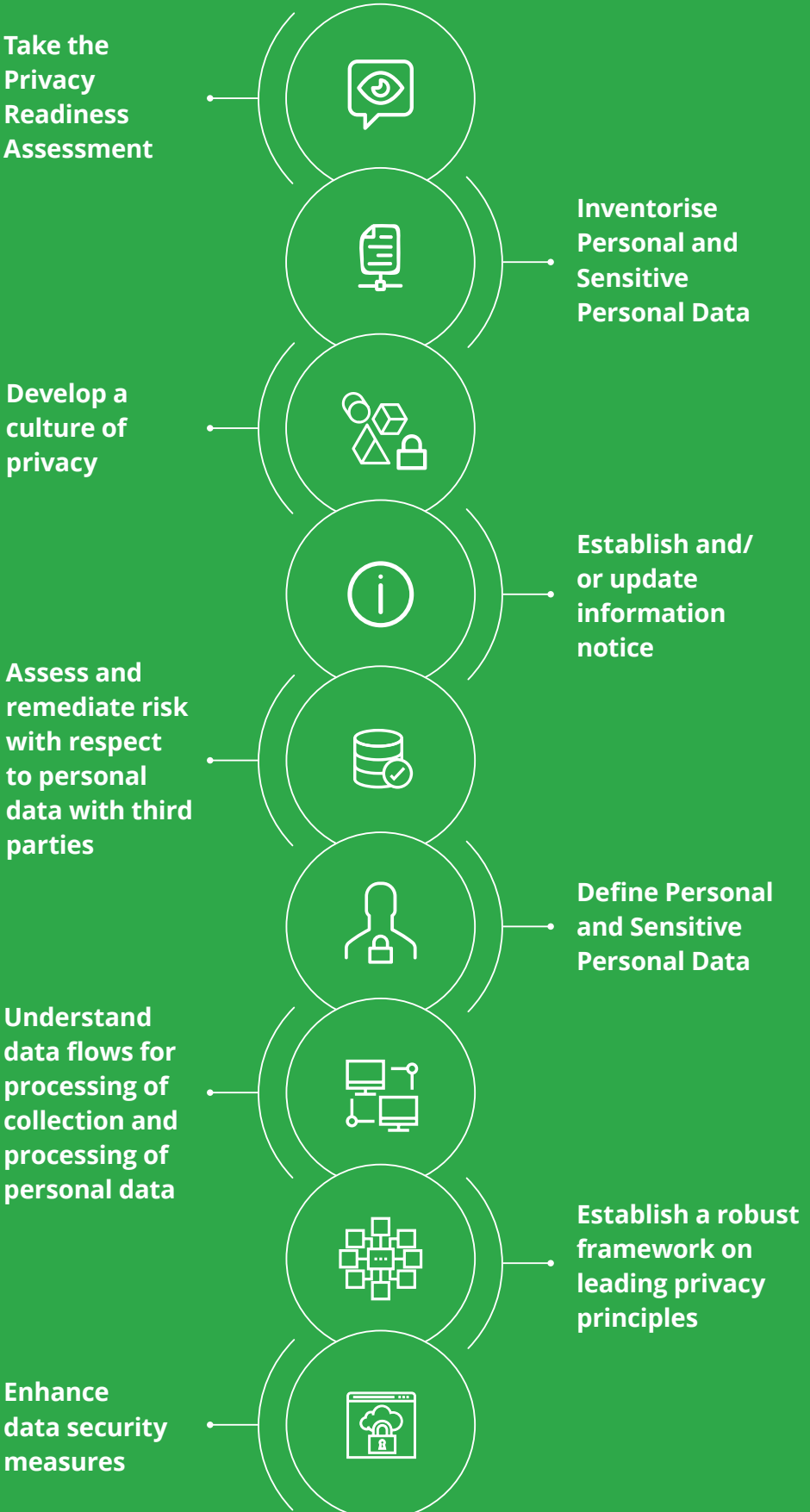
INR 5 cr or **2%** of global turnover, whichever is higher

- 01 Ground of processing of personal data
- 02 Ground of processing of sensitive personal data
- 03 Ground of processing of personal and sensitive personal data of children
- 04 Adhering to data security safeguards
- 05 Transfer of personal data outside India subject to defined conditions

What next?

A proactive approach

Until the law gets enacted, organisations may consider the following initiatives:



Glossary



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 processing of personal data



Data principal

The natural person to whom the personal data relates



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, but does not include an employee of the data fiduciary;



Personal data

Data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information

The Bill in brief



Data Protection Obligation

Personal data should be processed in a manner that is fair, and ensures privacy. It mandates collection and processing of personal data to be limited to a defined purpose



Processing of Personal Data

Six (6) grounds for processing - a) Consent b) Function of Parliament or any State Legislature c) Compliance with law or any order of any court or tribunal d) Prompt action (e.g. medical emergency involving a threat to the life disaster scenario etc.) e) Employment, and f) Reasonable purposes



Data Principal Rights

Individuals /or data principals may exercise - a) Right to confirmation and access b) Right to correction c) Right to Data Portability d) Right to Be Forgotten



Transparency and Accountability

To be achieved by appointing a Data Protection Officer and privacy fundamentals such as Privacy by Design, Information/ Data Security, Data Breach Notification, Impact Assessment, Record Keeping etc.



Cross border data flow

Organisations are expected to store a copy of personal data within India and transfer of personal data outside Indian territory is permissible, subject to conditions mandated by the bill

Privacy is a fundamental right and protecting the personal data of Indian data principal is at the core of the bill.

Key contacts

National

Rohit Mahajan

President
Risk Advisory
rmahajan@deloitte.com

Shree Parthasarathy

Partner
Risk Advisory
sparthasarathy@deloitte.com

Manish Sehgal

Partner
Risk Advisory
masehgal@deloitte.com

Regional

West - Ashish Sharma

Partner
Risk Advisory
sashish@deloitte.com

North - Gautam Kapoor

Partner
Risk Advisory
gkapoor@deloitte.com

South - Maninder Bharadwaj

Partner
Risk Advisory
manbharadwaj@deloitte.com

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

This material is prepared by Deloitte Touche Tohmatsu India LLP (DTTILLP). This material (including any information contained in it) is intended to provide general information on a particular subject(s) and is not an exhaustive treatment of such subject(s) or a substitute to obtaining professional services or advice. This material may contain information sourced from publicly available information or other third party sources. DTTILLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such sources. None of DTTILLP, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this material, rendering any kind of investment, legal or other professional advice or services. You should seek specific advice of the relevant professional(s) for these kind of services. This material or information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person or entity by reason of access to, use of or reliance on, this material. By using this material or any information contained in it, the user accepts this entire notice and terms of use.