Deloitte.

India Draft Personal Data Protection Bill, 2018 and EU General Data Protection Regulation

A comparative view

For Private circulation only

Risk Advisory

Contents

Overview of the Draft Personal Data Protection Bill, 2018 of India 04

Overview of the General Data Protection Regulation 05

Grounds for processing personal data 06

Grounds for processing sensitive personal data 06

Key requirements of Draft PDPB, 2018 to be considered by GDPR ready organizations 12

What it means for organizations 13

Overview of the Draft Personal Data Protection Bill, 2018 of India

What is Personal Data Protection Bill, 2018?

The Personal Data Protection Bill, 2018 ensures protection of individuals personal data and regulates the collection, usage, transfer and disclosure of the said data. The Bill provides access to data to the individuals and places accountability measures for organizations processing personal data and supplements it by providing remedies for unauthorized and harmful processing.

Applicability: In its current state the Bill is applicable to those organizations that are:

a. Processing the data that has been collected, disclosed or shared within the territory of India
b. 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
c. The bill is applicable to the processing of personal data if the same is undertaken by the State, any Indian company or any Indian citizen or persons incorporated under the Indian law.

This bill is a sectorless law and applies to all categories of industries.

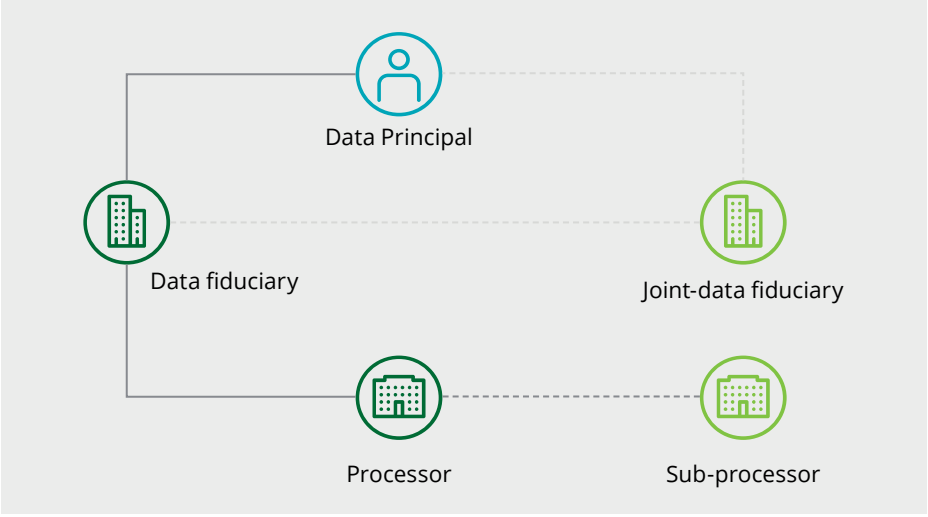
The terms Data Subject and Data Controller have been termed as Data Principal and Data Fiduciary respectively to highlight the nature of relationship between the two.

Roles provided under draft PDPB, 2018

Data Principal means the natural person to whom the personal data relates to.

Data Fiduciary means 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 Processor means 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.



Overview of the General Data Protection Regulation

What is General Data Protection Regulation?

The General Data Protection regulation was adopted by the European Commission and ensures protection of individual in relation to the processing of personal data. The Regulations provides for certain data subject rights, security safeguards and accountability measures that will need to be complied by the organizations.

Applicability: The Regulation is applicable to the processing of personal data that is wholly or partly performed by automated means. It is applicable to those organizations that are:

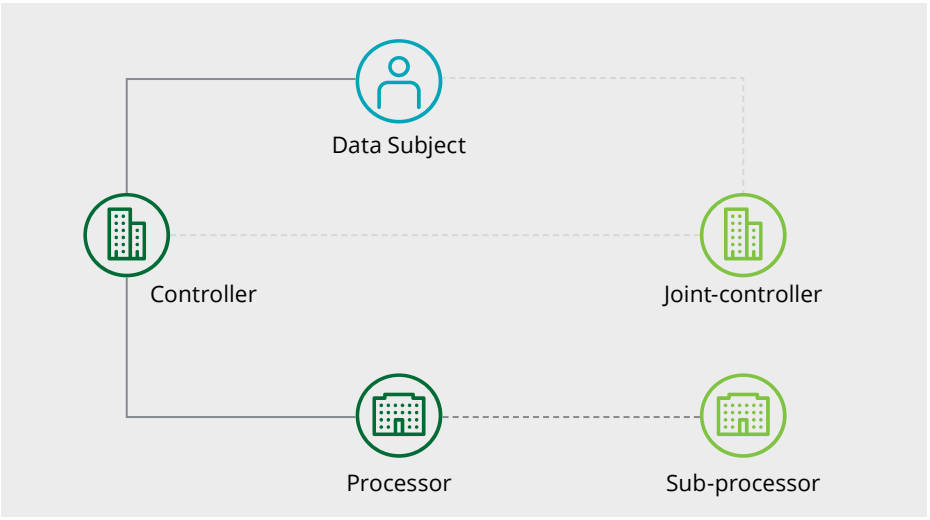
a. Present in the European Union (EU), regardless of whether the processing takes place in the EU or not.
b. Not established in the EU but are processing personal data of data subjects who are in the EU where the processing activities are related to the offering of goods or services or monitoring of behavior of such data subjects in the EU.
c. Not established in EU but are in a place where Member State law applies by virtue of public international law.

Roles provided under GDPR

Data subject means an individual who is the subject of personal data

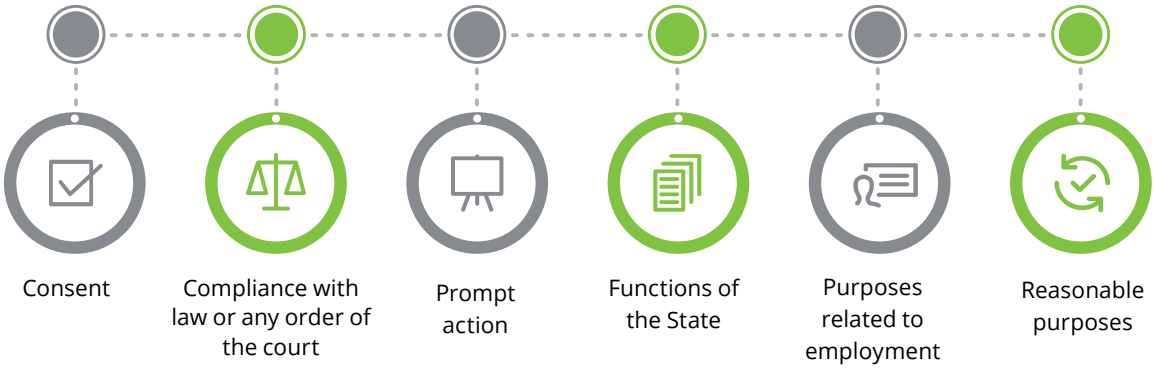
Controller means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data

Processor means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.



Grounds for processing personal data

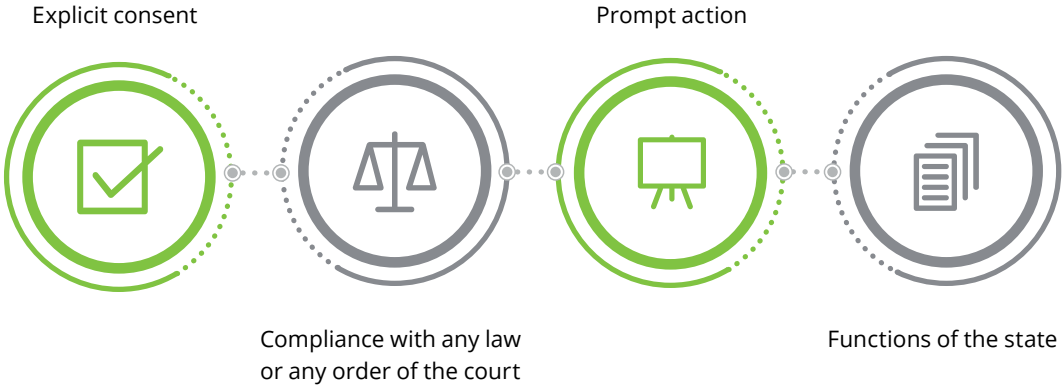
Draft PDPB, 2018



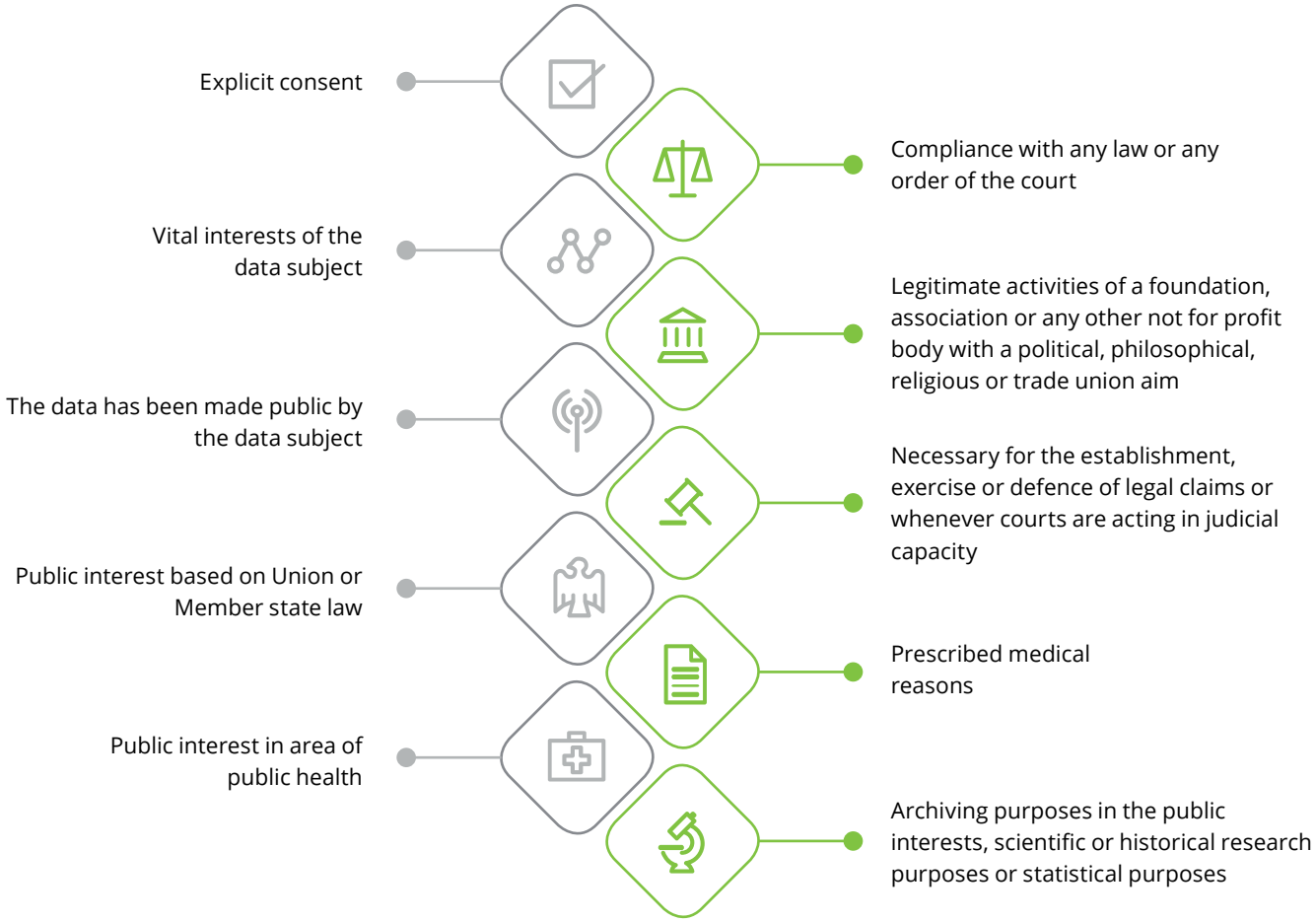
GDPR

Grounds for processing sensitive personal data

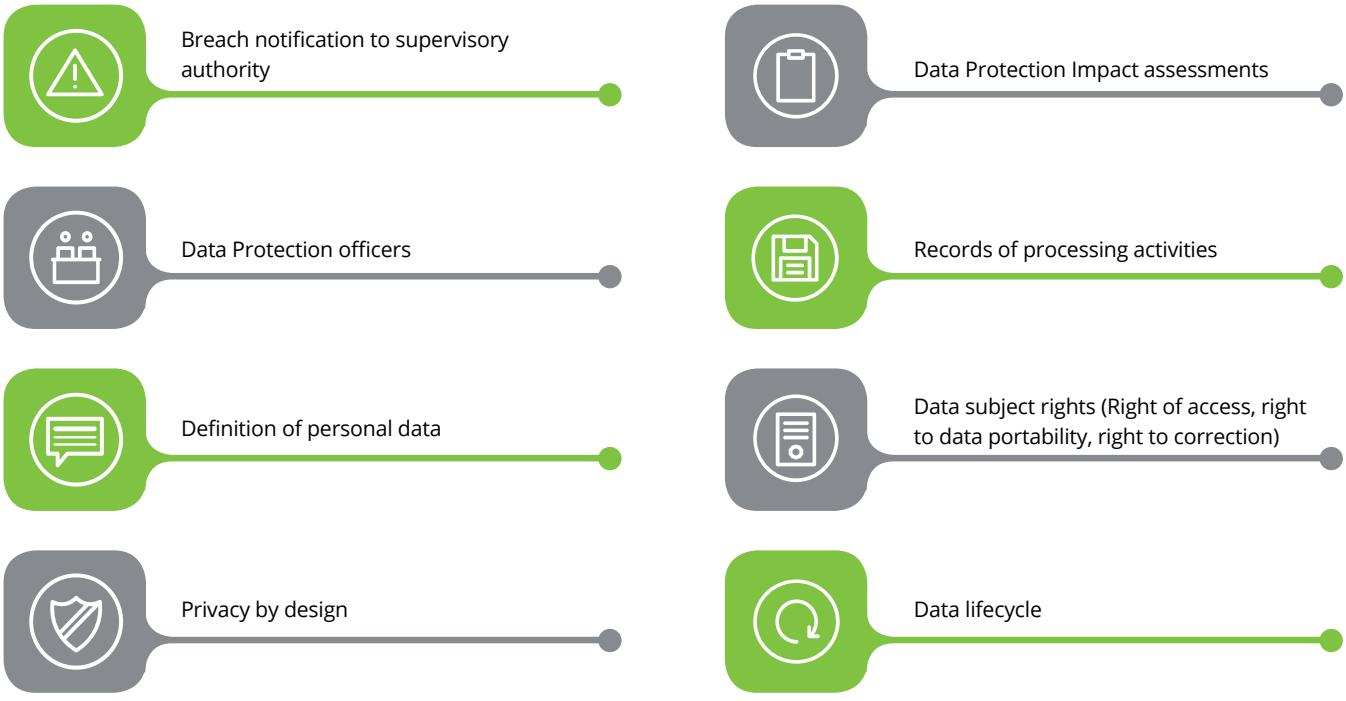
Draft Personal Data Protection Bill, 2018



General Data Protection Regulation



Common Key requirements for Draft PDPB, 2018 and GDPR



Differences between Draft Personal Data Protection Bill, 2018 and GDPR

	Draft PDPB, 2018	GDPR
Applicability	• The provisions of the Act apply to the processing of personal data within the territory of India and to the processing of personal data by the State, any Indian company, any Indian citizen or any person or body of persons incorporated under Indian law. • The extra territorial application extends to processing in connection with any business carried on in India or processing which involves profiling of data principals within the territory of India.	• The provisions of the Regulation apply to processing activities of an establishment in the EU regardless of whether the processing takes place in the EU or not. • The extra territorial application extends to processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU if the processing is related to the offering of goods or services or monitoring of their behavior.
Restriction on Cross Border Data Transfer	• Data fiduciaries transferring data outside the territory of India are required to maintain a serving copy of the data within the territory of India. • Categories of personal data that are notified as critical personal data by the Central Government can be processed only within the territory of India.	• GDPR doesn't require a serving copy to be maintained within the territory of the Member State.
Conditions for cross border data transfer	• Personal data may be transferred outside the territory of India pursuant to either one of the following conditions: – Adequacy decision by the Central government after consultation with the Authority – Standard contractual clauses or intra-group schemes approved by the Authority – A situation of necessity as determined by the Authority – Data subject's consent in addition to adequacy decision or the standard contractual clauses.	• The transfer of data to a third country or to an international organization is permissible pursuant to either one of the following conditions: – Adequacy decision by the European Commission (A list of countries is available with the Commission at present) – Binding corporate rules – Standard data protection clauses adopted by the Commission or the Supervisory Authority – Approved code of conduct – Approved certification mechanisms – Necessary for the performance or conclusion of a contract between data subject and controller – Necessary for public interest or to protect the vital interests of the data subject
Data principal/ subject consent for cross border data transfer	• The data principal's consent is needed in addition to the adequacy decision by the Central Government or the approved standard contractual clauses.	• In the absence of an adequacy decision by the Commission or of appropriate safeguards such as standard contractual clauses etc. personal data can be transferred to a third country if the data subject has explicitly consented to the said transfer.

	Draft PDPB, 2018	GDPR
Breach notification to data principal/	• The data fiduciary is not obligated to inform the data principal about a personal data breach unless and until the Data Protection Authority has mandated such reporting to the data principal.	• The controller should communicate the personal data breach to the data subject without undue delay in cases where the breach is likely to result in a high risk to the rights and freedoms of natural persons.
Breach Notification to Authority	• The time period for notification by the data fiduciary to the Authority in case of a personal data breach will be provided after the notification of the Bill in the Gazette.	• The controller must notify the Supervisory Authority in case of a personal data breach not later than 72 hours after becoming aware of the breach.
Sensitive personal data	• Trade union memberships, racial or ethnic origin and philosophical beliefs are not considered as sensitive personal data. • Passwords, financial data, transgender status, intersex status, caste or tribe, religious belief and political belief are considered as sensitive personal data in addition to the data mentioned in GDPR.	• Racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union memberships, genetic data, biometric data, health data, details of sex life and sexual orientation.
Personal Data	• The Central government shall categorize certain personal data as critical personal data which must be only processed in a server or data centre located in India.	• No such classification of data under the current provisions or guidelines.
Data Protection Officer	• The explicit responsibility of promoting awareness lies with the Data Protection Authority and not the Data Protection Officer. • The DPO can be assigned any other function if necessary by the data fiduciary.	• The Data Protection Officer is responsible for raising awareness, training the staff and related audits.
Data Protection Authority	• The Authority in India also has the power to specify reasonable purposes of processing, residuary categories of sensitive personal data, determine the criteria for a data trust score to be issued by the data auditor and provide certification for registration of data auditors.	• The primary function of the Data Protection Authority is to ensure compliance and promote awareness with respect to the provisions of the Regulation.
Right to be forgotten/Right to erasure	• A data principal can only restrict or prevent continuing disclosure of the personal data by the data fiduciary if the grounds for such restriction are fulfilled. No provision to erase personal data.	• A data subject has the right to obtain erasure of their personal data from the data controller if the grounds for such erasure under the Regulation is fulfilled.
Right to data portability	• Similar right of data portability as in GDPR. • However the right is restricted in cases where it would reveal a trade secret of any data fiduciary or would not be technically feasible.	• The data subject has the right to receive or transmit to another controller, the personal data provided in a structured commonly used and machine-readable format.

	Draft PDPB, 2018	GDPR
Right to object and automated individual decision making	• No such explicit right has been defined in the draft Bill as of now.	• The data subject has the right to object to processing of his personal data in certain cases.
Right to restriction of processing	• No such explicit right has been defined in the draft Bill as of now.	• The data subject has the right to restrict the controller from processing personal data provided in certain cases.
Data Audits	• The audits are to be conducted by an independent auditor in the form, manner and the procedure as prescribed by the Authority.	• The Supervisory Authority has the power to carry out investigation in the form of data audits.
Demonstrating compliance with the respective legislations	• The auditor provides a data trust score to the data fiduciary which indicates the state of compliance of the data fiduciary with respect to the provisions of the draft Bill.	• Establishment of data protection certification mechanisms and data protection seals and marks to demonstrate compliance with the Regulation will be encouraged by the Member States, supervisory authorities, the Board and the Commission.
Redressal	• The data principal can approach the data protection officer or the grievance officer with regard to issues related to the processing of data. In case of lack of efficient response, the data principal can approach the adjudicating officer to address any violations of the draft Bill.	• The data subject can approach the Data Protection Officer with regard to issues related to the processing of personal data. A data subject can lodge a complaint with the Supervisory Authority in case of any violation of the Regulation.
Penalties	• The fines under draft PDPB range from 2%-4% of the worldwide turnover or 5-15 crores rupees whichever is higher. • Certain offences under the draft bill are categorized as cognizable and non bailable.	• The administrative fines under GDPR range from 2%-4% of the worldwide turnover or 10-20 million Euro whichever is higher. • The offences under GDPR are not criminally sanctioned.
Enforcement Date	• The Draft PDPB, 2018 is not in force as of yet. The transitory provisions of the Bill give the organisations a period of 18 months from the enactment date to comply with the requirements of the Act.	• The provisions of the General Data Protection Regulation has been in force since 25th May 2018.
Exemption for Journalistic purposes	• For the exemption for journalistic purposes, the Draft PDPB relies on the ethics issued by the Press Council of India and any other media regulatory organization.	• For the exemption for journalistic purposes, GDPR relies on the balancing test between freedom of speech and expression and protection of personal data.
Exemption for Personal or domestic purposes	• Data processed in the course of a purely personal or domestic purpose is exempted from the provisions of the draft Bill except with the provision related to fair and reasonable processing.	• Data processed for a purely personal or household activity is exempt from the provisions of the Regulation.

Key requirements of Draft PDPB, 2018 to be considered by GDPR ready organizations

1

Restriction on cross border data transfer

Data fiduciaries are required to maintain a serving copy of the personal data being transferred outside the territory of India on a server or a data centre within India. Categories of personal data notified as critical personal data can be processed only within the territory of India

2

Cross Border Data Transfer

Data fiduciaries will have to obtain the data principal's consent in addition to the adequacy findings of the Central government or the standard contractual clauses or intra-group schemes approved by the Authority

3

Definition of Sensitive Personal Data

The definition of sensitive personal data under the Draft PDPB, 2018 has been expanded to include passwords, financial information, intersex status, intersex status, caste or tribe, religious belief and political belief.

4

Grounds for processing of personal data

The Draft PDPB, 2018 doesn't consider a contractual relationship with the data principal as a ground for processing of personal data. Data fiduciaries relying on the contractual relationship will have to modify their policies to process personal data based on the other lawful grounds under the draft Bill.

5

Guardian Data Fiduciaries

Data fiduciaries notified as guardian data fiduciaries shall be barred from profiling, tracking or behavioral monitoring or targeted advertising directed at children.

What it means for organizations

The requirements of the Draft PDPB, 2018 emulate the privacy principles incorporated under GDPR. However, there are certain additional procedural requirements that organizations will need to comply with if their processing activities fall under the applicable scope of the draft Bill. An assessment of the current policies and practices must be conducted to identify gaps specific to the draft PDPB, 2018.

Contacts

Rohit Mahajan
President
Risk Advisory
rmahajan@deloitte.com

Shree Parthasarathy
Partner
sparthasarathy@deloitte.com

Manish Sehgal
Partner
masehgal@deloitte.com

Deloitte.