MGC
GLOBAL RISK ADVISORY LLP

## PERSONAL DATA PROTECTION BILL


The transfer and security of the twenty first century's gold- 'data' is at the center of global deliberations. Following the implementation of General Data Protection Regulation ('GDPR') in May of 2018, the government of India ('the Government') has taken a significant step to enact a similar legislation, which has been tabled before the Parliament in the form of the Personal Data Protection Bill, 2019 ('PDPB' or 'the Bill'),

**Who does the Bill apply to? What is the impact of PDPB on organizations in India? What are the consequences of not complying with the Bill once it is enacted? What are the main differences between PDPB and GDPR? How should organizations in India prepare to embrace this change?**

This publication from MGC Global Risk Advisory's Thought Leadership Series provides the perspectives of our IT services team of experts on these and other burning questions.

### Applicability

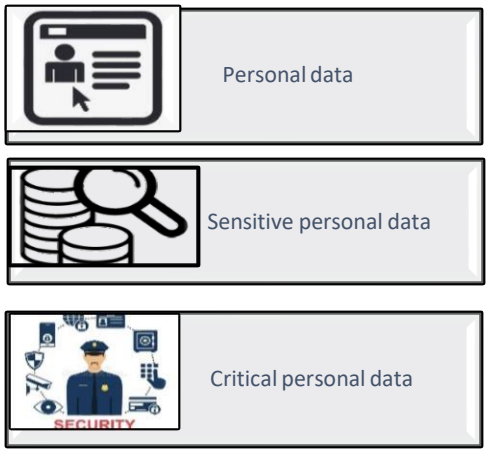
The Bill, which deals with the manner in which organizations collect, store and process data, extends to both private and government bodies.

The applicability of the Bill is extended to data controllers/trustees or data processors who are not present within the territory of India and where the processing of personal data

- Is carried out in connection with any business being carried out in India;
- Involves profiling of data within the territory of India; &
- Entails a systematic provision of goods and services on data principles in India.

Processing of such data is allowed only when; an individual gives consent; & in case of a medical emergency or by the State for providing benefits.

**The Bill trifurcates data in the following three categories:**




### Impact on organizations

#### Imposition of restrictions on data localization requirements…

While data typically can by-pass borders without any restrictions, some constraints have been built in, with limits on "sensitive personal data" that need to be stored in India and which can only be processed overseas after approval from the Regulator. For "critical personal data", that the Government classifies on its own, there are hard restrictions and this data needs to be both stored and processed within India.

#### The need for technical security safeguards…

Technical security safeguards, including de-identification *(preventing an individual's identity to be inadvertently revealed)* and encryption needs to be built in. Larger organizations *(depending on the volume of data, annual turnover and other factors*) and social media companies with users above a defined threshold will have additional responsibilities.

### Privacy by design policy…

Organizations need to plan and adopt a “privacy by design" policy, denoting that user privacy should be at the heart of the engineering model all the way through the the growth cycle of product development and as such should not be retroactive. The regulator will attest and authorize the policy cantered on prerequisite standards.

### The Government has the authority to solicit anonymized or non-personal data from companies…

The Government can ask organizations to provide “anonymised “or “non-personal data" for policy making or other public goods. The intent is to use aggregated data to derive meaningful insights and unknown trends.

### The rules do not apply to processing of anonymized data, leaving it to the decision of the regulator…

Organizations can continue to identify localities, which say, mostly buy a particular regional cuisine or those that do not order non-vegetarian food at all or those that order holy scriptures of specific religion or clothes of a certain kind. While none of these may reveal anything about an individual however the data points can portray specific aspects about a community.

### Proposition of stiff penalties…

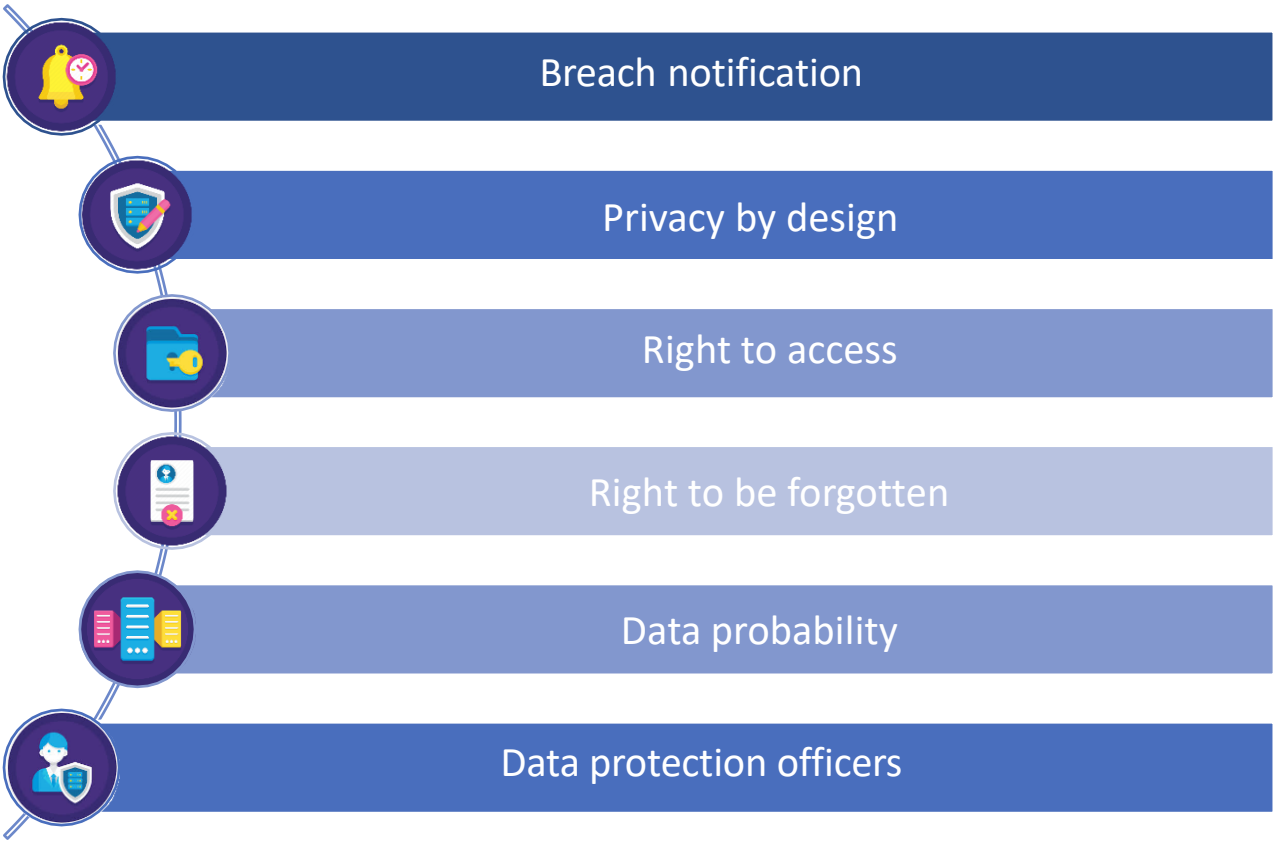
**4% of an organization’s total turnover**

**or**

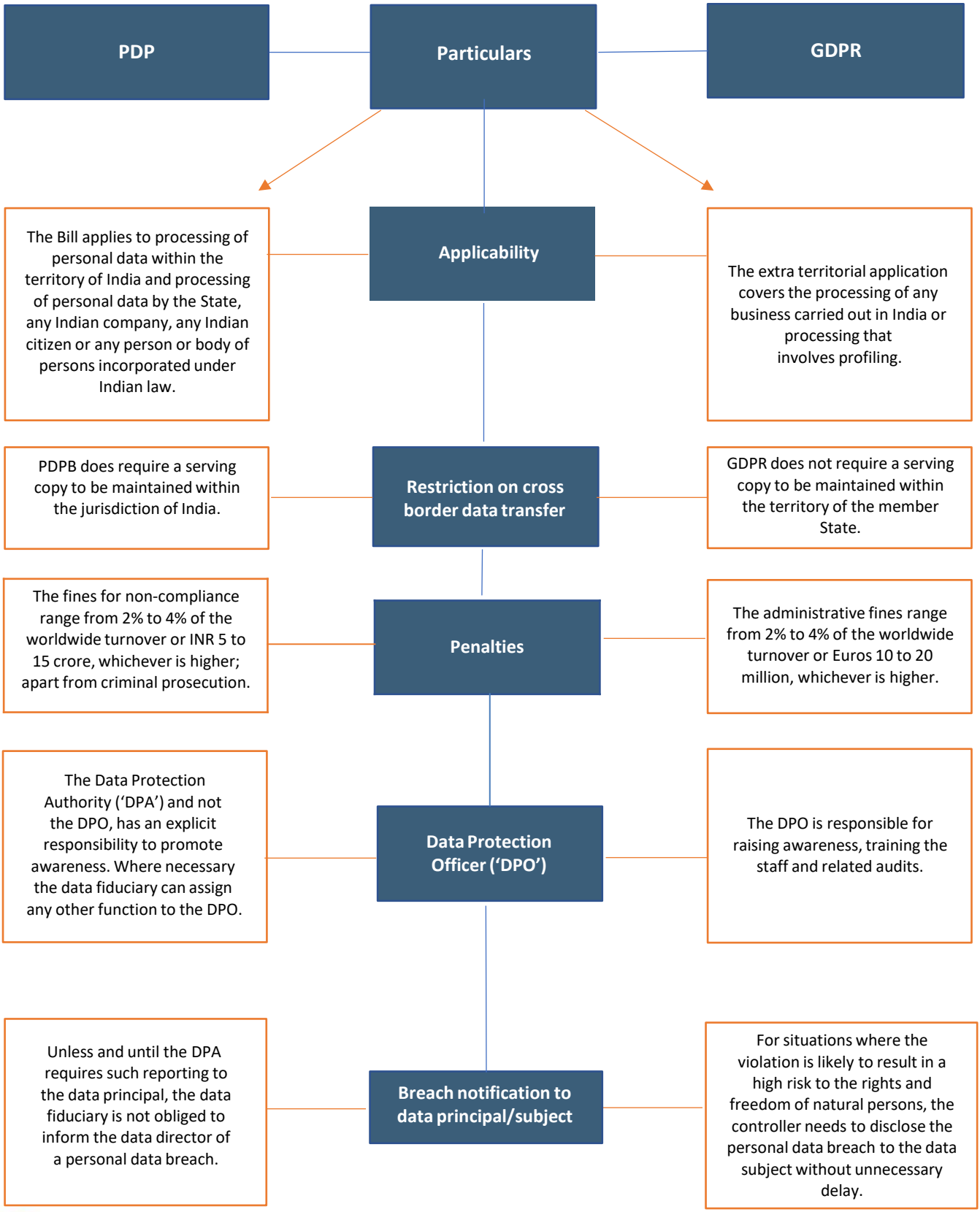
**Up to INR 15 crores**

## Requirements

The primary requirements of the Bill include six areas:



## PDPB and GDPR | Presenting the polarity:



| PDP | Particulars | GDPR |
|---|---|---|
| Personal data may be transferred outside India under either of the following conditions:<br>• Adequacy decision of the Government after consultation with the authority;<br>• Standard contractual clauses or intragroup schemes approved by the regulator;<br>• Condition of need as decided by the regulator; &<br>• Consent of the data subject in addition to adequacy decision. | Conditions for cross border data transfer | The transfer of data to a third country is permissible pursuant with either one of the following conditions:<br>• Adequacy decision by the European commission;<br>• Binding corporate rules;<br>• Standard data protection clauses adopted by the commission or the supervisory authority;<br>• Approved code of conduct;<br>• Approved certification mechanisms;<br>• Necessary for the performance or conclusion of a contract between data subject and controller; &<br>• Necessary for public interest or to protect the vital interests of the data subject. |
| In addition to the Government's adequacy decision or the accepted standard contractual provision, consent of the data principal is required. | Data principal/subject consent for cross border data transfer | In the absence of a commission decision on adequacy or adequate safeguards such as standard contractual clauses etc., personal data may be transferred to a third country where the data subject has been explicitly consented. |
| After notification of the Bill in the Gazette, the time limit for notification by the data fiduciary to the authority in the event of a personal data breach will be given. | Breach notification to authority | 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. |
| The Government shall categorize such personal data as sensitive personal data that must only be stored in an India based server or data center. | Personal data | No such classification of data under the current provisions or guidelines. |

| PDP | Particulars | GDPR |
|---|---|---|
| Trade union memberships, racial or ethnic heritage, and philosophical beliefs are not regarded as sensitive personal information. 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. | Sensitive personal data | Racial or ethnic origin, political views, religious or philosophical beliefs or trade union memberships, genetic data, biometric data, health data, sex-life details and sexual orientation. |
| The revised PDPB is not yet in effect. The Bill's transitory clauses grant organizations 18 months from the date of enactment to meet the requirements of the Act, to be given by the data auditor and the qualification for data auditors ' registration. | Enforcement date | The provisions of the GDPR have been in force since May 25th, 2018. |
| There is a 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. | Right to data portability | The data subject has the right to receive or transfer on the personal data given to another controller in a widely used standardized and computer readable format. |
| No such explicit right has been defined in the draft Bill as of now. | Right to object and automated individual decision making & right to restriction of processing | The data subject has the right to object to processing of his/her personal data in certain cases. |
| A data principal can restrict or prevent the data fiduciary from continuing disclosure of personal data only when the grounds for such restriction have been satisfied. No provision for deleting personal data. | Right to be forgotten/ right to erasure | 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. |

## Conclusion…

A legislation to protect data in India was inevitable *(and even necessary)* given the growing digital footprint of users and the scattered trail of sensitive data they leave behind, such as the internet, storage media and other unforeseen obstacles such as ambient data in devices where data could be processed without the user's permission or consent. The Bill is a step forward in meeting the requirements of India's changing data protection system.

The Bill actually contemplates that the clauses will come into force on the day they are published in India's official gazette *(which will take place upon ratification by the Indian Parliament and the President of India).*

Organizations in India would need to prepare for compliances in the PDPB by establishing the sources of information, mapping the flow of the same with the touch points, measures to obtain, store, retrieve and destroy the information and develop a robust set of procedures covering the value chain of activities related to data protection.

We are hopeful that the Bill, in its final form, will provide companies sufficient time to conform their business practices to ensure compliance with the same in substance and form.

**How can we help you?**

- Maturity assessment – assessing the impact of the legislation on your current state;
- Development of policies, procedures, IT solutions to meet compliance requirements;
- DPO and data fiduciary services;
- Conduct of GDPR and PDPB awareness workshops;
- Spearheading privacy by design implementation;
- Data branch notification & incident management services;
- GDPR audits & reviews;
- Undertaking GDPR transformation programs;
- Data processing inventory services; &
- Conducting third party procedures.

*For expert assistance, please contact:*
***Lalit Sharma*** *| lalit.sharma@mgcglobal.co.in |*
***Gautham Desai*** *| gautham.desai@mgcglobal.co.in |*
***Aditi Mishra*** *| aditi.mishra@mgcglobal.co.in |*
*Visit us at: www.mgcglobal.co.in*

**MGC Global Risk Advisory LLP ('MGC Global' or 'the Firm')**

Recognized as one of the '10 most promising risk advisory services firms' in 2017, as the 'Company of the Year' in 2018 &, 2019' *(both in the category of risk advisory services),* one of the 'Top Exceptional Companies to Work For' in 2020, amongst the 'Top 25 Customer Centric Companies' in 2020 and 'The Consultant of the year' in 2021 *(in the category of risk advisory services);* MGC Global is an independent member firm of the US$ 4.2 billion, Atlanta headquartered - Allinial Global.

MGC Global provides services in the areas of enterprise wide risk management, control assessments *(SOC, IFCR & SOX)*, internal audits, process re-engineering, governance frameworks, IT risk advisory, GDPR, cyber security, CxO transformation and forensic services. Our Firm has the capabilities to service its clients through its offices in Bengaluru, Mumbai, NCR; and has service arrangements in all major cities in India.