Draft PDPB & EU – GDPR

Applicability of PDPB

The objective of the bill is to ensure a free and fair digital Indian economy and it is seen as an critical step in setting up a privacy framework which gives the Indians full freedom to protect their personal data.

Any Indian company, Indian citizen or person or body of persons...

....involved in processing of personal data.

Parameters for establishing applicability	
Establishment in India	Processing of personal data where such data has been collected, disclosed, shared or otherwise processed **within the territory of India**
Establishment in India	Processing of personal data by the State, any Indian company, any Indian citizen or any person **or body of persons incorporated or created under Indian law**
Offering goods and Services	Processing of personal data by data fiduciaries or data processors **not present within the territory of India**, but the processing is related to-any **business carried on in India,** or any systematic activity of offering goods or services to data principals within the territory of India
Behavior monitoring	Processing of personal data by data fiduciaries or data processors **not present within the territory of India**, but the processing is related to any activity which involves **profiling of data principals within the territory of India.**

Personal Data Protection Bill- Quick snapshot

Applicability – Who will be impacted ?

- Indian company
- Indian citizens
- Government agencies
- Person or body of persons created under the Indian Law
- Personal data processed within territory of India
- Systematic activity of offering goods and services to principals within India
- Activity involving profiling of data principals* in India

Types of data considered in the bill

Personal Data
Data about or relating to a natural person who is directly or indirectly identifiable

Sensitive Personal Data
such as financial , health data, official identifier, sex life, intersex status, caste, tribe, religious, political views, genetic/biometric data or other data categorized sensitive by the authority
Transfer outside India-with explicit consent, contract/intra-group scheme or allowed by Central Govt.

Critical Personal Data
Data type to be specified by the central Govt. from time to time
Transfer outside India under exceptional cases only

Tough Penalties

Fines up to

2%-4% or INR 5-15 crores

of total worldwide turnover whichever is higher

Imprisonment and /or fines

3 years and / or INR 2 lakh

For reidentification and processing of deidentified personal data

Key Highlights of the Bill

Provide clear notice and consent for collection and processing of personal data.
Consent manager to enable data principals to withdraw, review and manage consent.

Notify the authority of any personal data breach likely to cause harm to any data principal

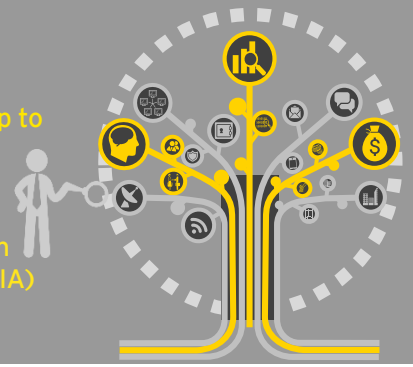
Products, systems and processes must consider privacy-by-design concepts during development and submit the policy to the authority for certification

Social media intermediary introduced to allow interaction between two or more users and allows them to create, upload, modify or access information using its services

Authority will be making a Sandbox available for innovation in AI, ML, and other technologies

Data principal rights- rights to correction, right to confirmation and access, right to portability and right to be forgotten.
Data principals have adequate grievance redressal procedure.
Data fiduciary* to resolve complaints within 30 days

Central government may frame policies for digital economy in respect of non personal data



Maintain accurate and up to date records as per requirements

Conduct Data Protection Impact Assessment (DPIA) under select conditions

Data Fiduciary should take steps to maintain transparency regarding general practices relating to processing of personal data.

Significant Data Fiduciary

Data Authority could classify certain entities as 'Significant Data Fiduciary' based on factors such as a number of users, the volume of data, the sensitivity of data and turnover of data

Additional obligations of significant data fiduciaries

- Register with the Data Protection Authority (DPA)
- Undertake data protection impact assessments (DPIA) for high risk processing and maintain data records
- Appoint a data protection officer (DPO)- based in India
- Get the privacy policies and the conduct of processing of personal data audited annually by an independent data auditor

Personal Data Protection Bill- Key Requirements

- All personal data, sensitive personal data and children data stored should be obtained by Consent
- Data Fiduciary should take steps to maintain transparency Follow principles of record keeping, data audits, Data Protection Impact Assessment and prepare a privacy by design policy.
- A data auditor ; an independent auditor has been proposed and Appoint a data protection officer
- The central government shall consult with sectoral regulator to notify categories of personal data as sensitive personal data.
- Any finding pertaining to transfer of personal data outside India shall be reviewed periodically
- Authority shall create a sandbox for encouraging innovation in field of AI, ML etc.
- Data fiduciaries shall be required to prepare a privacy by design policy
- Notification pertaining to a breach shall be provided to the Authority by means of a notice
- Sensitive personal data can be transferred outside for processing but has to be stored in India based on consent provided by data principal; pursuant to a contract or intra group scheme approved by the authority;
- Critical data can now be transferred outside India based on two conditions ; provision of health services or emergency services ; Government has deemed the transfer permissible
- Data Trust scores for data fiduciaries by auditors
- Rights to data portability ; correction & erasure ; to be forgotten
- Category of significant data fiduciaries

In order to comply with the requirements of the bill, the organizations need to -

UNDERSTAND

Understand the impact of the PDPB on their organisation, broken down into business areas and both current and future projects

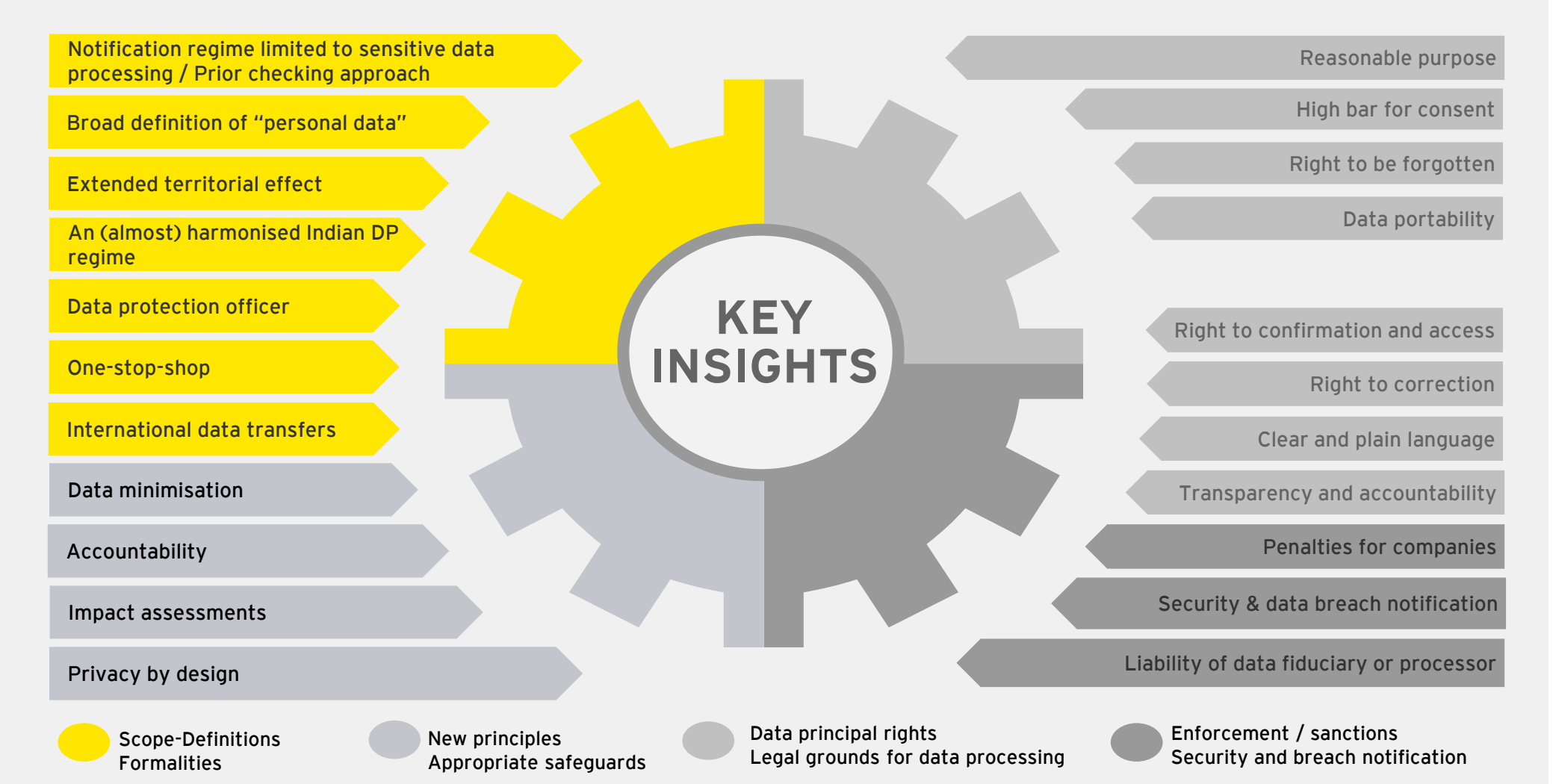
ASSESS

Assess the impact and prioritise actions to be taken in order to ensure PDPB compliance in an effective way.

ROADMAP

Set up a roadmap for implementing remediation actions to ensure full PDPB compliance.

Personal Data Protection Bill Insights



Key Considerations for Privacy Implementation

Embrace privacy by design
in all aspects and embed it in the DNA of the organization

Manage data breaches
Build capability to detect, analyse and contain data breaches

Revisit consent
User consents at all PI touch-points

Manage user rights
Build capabilities to cater to rights to individuals providing data (right to confirmation , access, correction, right to be forgotten and portability)

Conduct Data Privacy Impact Assessment
Conduct privacy impact assessments to identify, assess and mitigate or minimise privacy risks with data processing activities

Third Parties
Consider data privacy aspects while dealing with third parties

Limit storage of data
Identify the retention periods of personal data and conduct regular reviews to ascertain the need to retain personal data

Regulatory Landscape
Understand and comply with the requirements of the applicable data privacy regulations

Employee Awareness
Educate employees on the importance of data privacy

Incorporate adequate data handling practices
Examine every facet of data handling in the organization ensure purpose limitation, collection limitation, and lawfulness of processing

Enhance accountability of PI
Transform privacy governance and enhance accountability of personal data handled

Reinforce personal data security measures
Revisit existing security safeguards and implement additional controls for adequate protection of PI

Key areas analysis PDPB and EU GDPR

Key areas and summary analysis

Key Similarities & Differences

Below mentioned are some of the key similarities and differences between GDPR and Indian – Draft Personal Data Protection Bill

Similarities

Penalty: India has proposed that any company that fails to comply with the law will be fined Rs5 crore ($727,450) or 2% of its turnover, whichever is higher. The severity of this punishment mirrors that of the GDPR, which fines companies €20 million ($23 million) or 4% of turnover.

Consent: Consent will be the primary ground of processing available to most entities, as per Section 12 (Chapter III). This consent is required to be free, informed, specific, clear and, in an important addition, capable of being withdrawn.

Rights of Data Subjects / Principals: These include the right to access and correction, the right to data portability

Privacy by Design, DPIA and other security requirements: This also includes transparency obligations, conducting Data Protection Impact Assessments, audits and implementing security controls including encryption of data etc.

Data protection officer & governance: Need for a governance mechanism including appointing a Data protection officer to resolve the DPA / Supervisory authority queries , data principal / subject complaints etc.

Data minimization and Lawful processing: Purpose and collection limitation to personal data and processing to be done lawfully.

Records of Processing, Purpose and Transparency: Need to limit to the purpose, establish transparency and keep a records of the processing to establish a legal basis.

Differences

Right to be forgotten: It does not allow Indians to ask companies to completely delete data they have shared, an accepted practice in the EU. The "right to be forgotten" suggested in the bill only allows individuals to restrict companies from using their data.

Cross Border Data Transfer: As per Data protection bill, it needs all the personal data copy to reside in India premises, where as GDPR only requires you to have a local representative.

Criminal Liabilities: Non bailable offense charged for obtaining, transferring, or selling personal data in violation of the law as per Data protection bill, where as in GDPR there are no criminal liabilities listed explicitly.

Terminologies: Data controller is referred as Data fiduciary and Data subject is referred as Data Principal.

Data breach notifications: The notifications to the DPA are to be made only if the breach is likely to cause 'harm' to the data principal.

Thank You