Indian data protection regime – Close to reality?

Personal Data Protection Bill, 2018

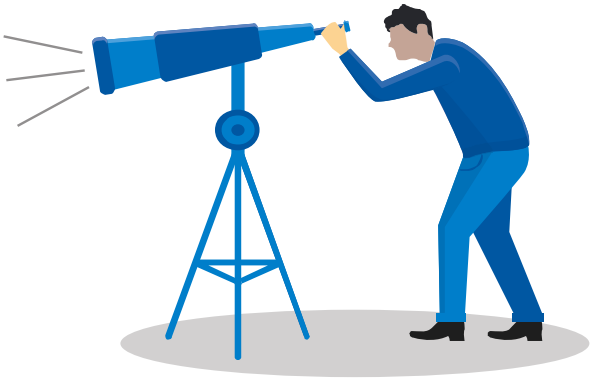
Overview

India has taken another step towards realising its dream of becoming a truly digital economy. Nearly a year after the landmark judgement by the Supreme Court of India that declared privacy as a fundamental right, the 'Justice BN Srikrishna Committee' (the Committee) released its first draft of the Personal Data Protection Bill (PDPB or the bill) on 27 July 2018.

The very usage of the word 'fiduciaries' in the proposed bill shows that its intent is to build a 'trust based relationship' between the data fiduciaries (similar to a data controller in GDPR) and the data principals (individuals whose personal data is being processed, similar to a data subject in GDPR).

The Committee considered the evolving and liberal nature of the data economy and thus, extended the territorial scope to ensure that even organisations, not physically located in India but offering goods and services in India, are regulated under the PDPB.

The organisations are to be granted a transition period of 12 months after the enactment of PDPB to become compliant.



Key highlights of the bill

1. Data protection obligations maintaining transparency, record keeping, conducting DPIAs, appointing a Data Protection Officer (DPO), timely notification of breaches etc. imposed on the organisation (called data fiduciaries/data processors) processing personal data of Indian residents (called data principals)
2. Legal grounds on which the personal data and sensitive personal data of Indian residents (including children) could be processed defined. While the bill firmly places the burden of proof for identifying the applicable legal grounds on the data fiduciaries, it also provides a wide berth to processing operations performed by the state
3. Rights provided to the data principals to give them the ability to control their personal data, which is being processed by the data fiduciaries, through rights such as the right to data portability and the right to be forgotten, similar to the ones provided to a data subject under GDPR
4. Measures such as privacy by design, notice, de-identification and encryption suggested to put in place for the data fiduciaries while processing personal data of the data principals to ensure transparency and accountability. While Indian organisations are at an equal footing with global standards for ensuring security of the data they process, realisation of concepts such as privacy by design may require additional time and resource cost
5. Data localisation introduced in the bill that mandates a copy of the personal data to be stored in servers/data centres in India. Certain categories of data (to be notified by the central government/ DPAI) termed as critical personal data shall only be processed in a server or data centre located in India

6. Fines and penalties suggested on individuals/ organisations found to be non-compliant with PDPB. The non-compliance may result in fines of up to 2-4 per cent of the global turnover or INR50-150 million (whichever is higher). Besides, non-adherence to the timelines specified for resolution of data principal rights will result in penalty of INR5000 for each day during which such default continues, up to INR10 lakh

7. Establishment of a Data Protection Authority of India (DPAI) and Appellate Tribunal by the central government has been suggested. A dedicated appellate tribunal could ensure fast resolution of issues and complaints received by the authority. However, the authority will have to proactively provide guidance on various issues which organisation may encounter in order to be compliant with the bill.

Components of personal data and sensitive personal data[1]

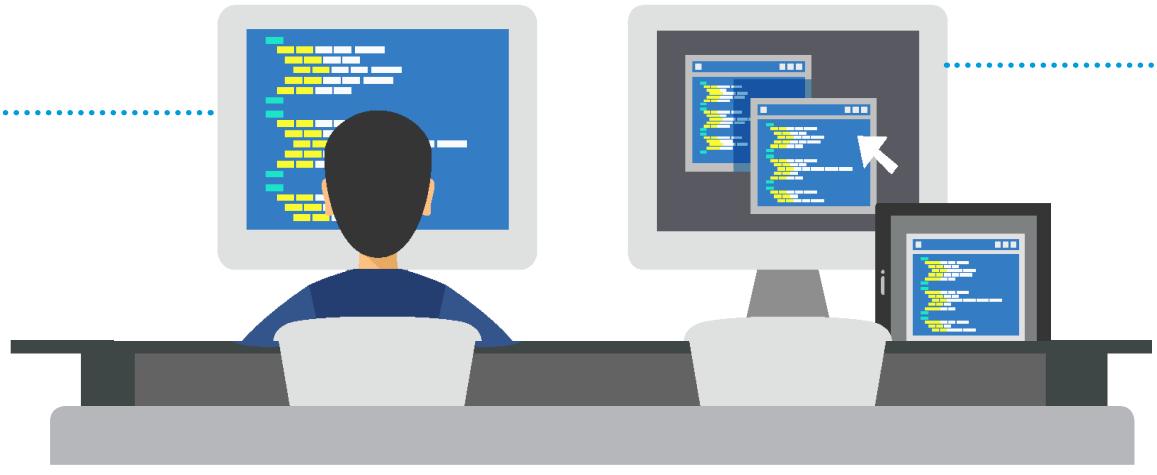
Sensitive personal data

Personal data revealing, related to, or constituting, as may be applicable:

- Passwords
- Financial data
- Health data
- Official identifier
- Sex life
- Sexual orientation
- Biometric data
- Genetic data
- Transgender status
- Intersex status
- Caste or tribe
- Religious or political belief or affiliation
- Any other category of data specified by the Authority under section 22.

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



1. The Personal Data Protection Bill 2018, Government of India, July 2018

What organisations must do to be compliant with PDPB

Organisations need to create a robust privacy framework consistent with the obligations specified under PDPB. The bill categorises organisations as Data Fiduciaries (DF) and Significant Data Fiduciaries (SDF) (to be notified by the DPAI) and imposes the following obligations on them:

Data Protection Officer- DPO (SDF)

The Data Fiduciary shall appoint a Data Protection Officer in India (irrespective of whether a Data Fiduciary has an establishment in India or not) to carry out the functions specified under PDPB. This involves providing advice to Data Fiduciary on fulfilling its obligations under PDPB, monitoring operations related to processing of personal data of data principals, maintaining inventory of all records, acting as a point of contact for DPAI and Data Principal's grievance redressals etc

Data Protection Impact Assessments (DPIA) (SDF)

If the Data Fiduciary intends to undertake any processing involving new technologies or large scale profiling or use of sensitive personal data such as genetic data or biometric data, or any other processing which carries a risk of significant harm to data principals, the Data Fiduciary must undertake a DPIA

Record keeping (SDF)

All Data Fiduciaries (including the state) need to maintain accurate and up-to date records of important operations in the data life cycle to demonstrate compliance with the obligations under PDPB

Contractual requirements with data processors

Data Fiduciaries to engage a data processor to process personal data of data principals on its behalf, only through a valid contract

Privacy by design (DF and SDF)

Data Fiduciaries to implement policies and measures to ensure that their processes and systems are designed in a manner to anticipate, identify and avoid harm to the data principals

Maintain transparency (DF and SDF)

Data Fiduciary to take reasonable steps to maintain transparency regarding its general policies related to processing personal data and make the information (as specified under PDPB) available in an easily accessible form

Timely notification of personal data breaches (DF and SDF)

Data Fiduciaries must notify the DPAI about any personal data breach as soon as possible within the timelines specified by the DPAI

Data audits (SDF)

Data Fiduciaries to have their policies and conduct of processing of personal data audited annually by an independent data auditor

Provide mechanisms for grievance redressal (DF and SDF)

Every Data Fiduciary to put in place proper procedures and effective mechanisms to address grievances of data principals efficiently and expeditiously within a period of 30 days

Other obligations include the following

- Proof of consent (DF and SDF):
  Where consent is an essential component of processing, the Data Fiduciaries must obtain valid consent from the Data Principals and ensure that they have mechanisms in place to showcase the obtained consent
- Facilitating data principal's requests (DF and SDF):
  Data Fiduciaries must facilitate the data principals in exercising their rights provided under PDPB
- Register with the DPAI (SDF):
  The Significant Data Fiduciaries are required to register themselves with the DPAI in the manner that will be specified by the DPAI.

Cross border transfers

The bill has emphasised on regulating cross border transfer of personal data and has imposed restrictions and conditions which needs to be adhered to, while transferring personal data of data principals outside India. Multinational organisations, in particular, will have to reconsider their Data Management practices and come up with measures to abide by these restrictions and ensure compliance to the conditions set in the bill. Some of the key restrictions include:

1. At least one serving copy of personal data is stored on a server or data centre located in India
2. Critical personal data (to be notified by the Central Government) is only processed via a server or data centre located in India.

Besides, the bill proposes the following key conditions on the transfer of personal data (provided the personal data does not fall under the restricted category):

1. The transfer be made subject to standard contractual clauses (approved by DPAI) and the data principal has provided his/her consent or explicit consent (in case of sensitive personal data) to such transfer
2. Personal data can be transferred to a country which is prescribed by the Central Government, and if the data principal has provided his/her consent or explicit consent (in case of sensitive personal data) to such transfer
3. A particular transfer or set of transfers of personal data is approved by DPAI due to a situation of necessity.

The bill takes into account emergency situations that might require a cross border transfer of personal data and, hence, allows transfer of sensitive personal data outside India when it is required for provisioning of physical well-being or any emergency services.

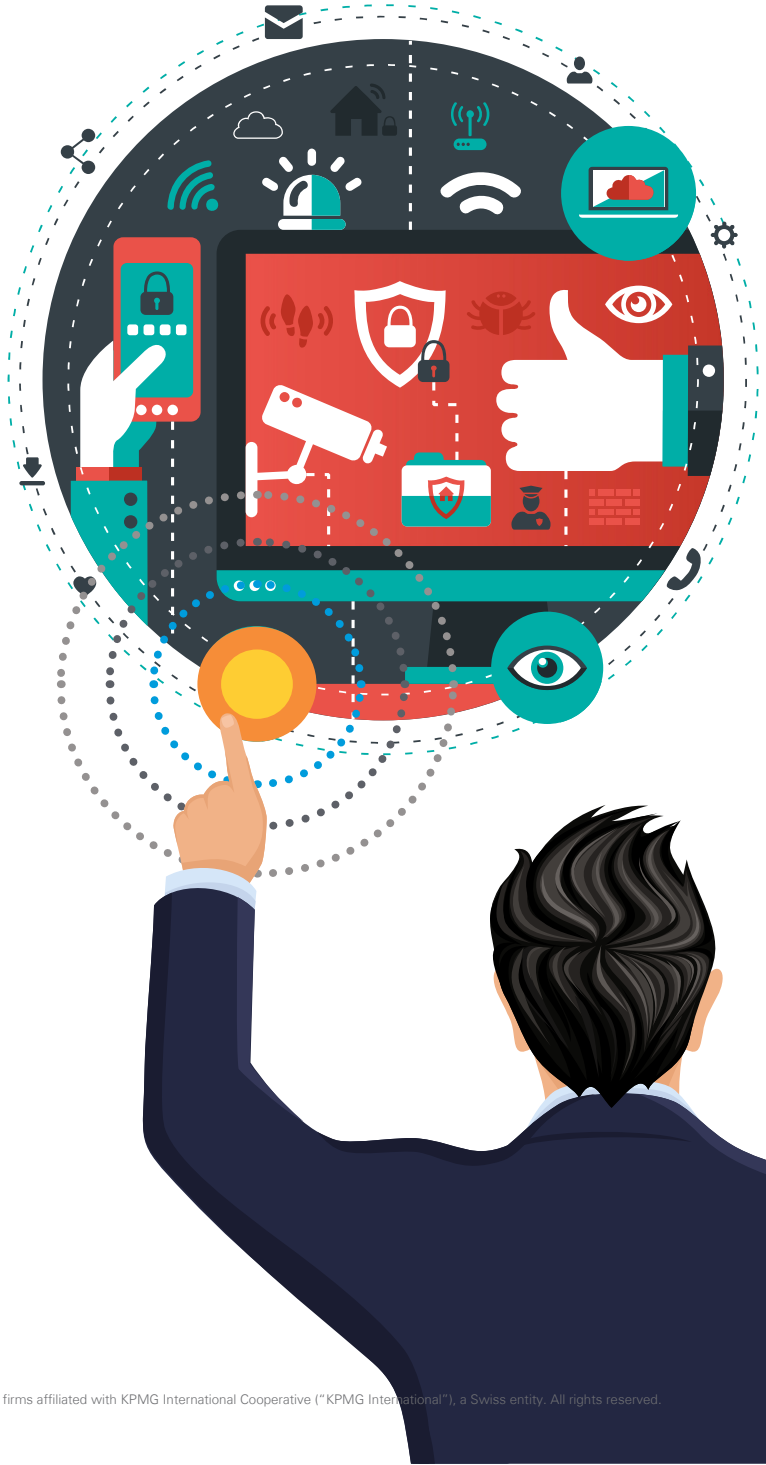
PDPB in comparison to GDPR

The core concepts of GDPR get reflected in the proposed PDPB. Some key similarities include (but not limited to):

1. The Data Controller, Processor and Data Subject roles under GDPR have been termed as Data Fiduciaries, Data processors and Data Principals respectively
2. The core principles of GDPR such as 'Lawfulness, Fairness and Transparency', 'Purpose Limitation', 'Collection Limitation', 'Data Quality', 'Storage Limitation', and 'Accountability' formulate part of the proposed PDPB as well
3. The definition of individuals under PDPB extends to the residents as well as the citizens, similar to the definition of a natural person under GDPR
4. The major rights of the data subjects under GDPR such as 'right to correction', 'confirmation and access', 'right to portability' and 'right to be forgotten 'will be extended to the data principals under PDPB too
5. Obligations on data fiduciaries on maintaining records of processing, conducting DPIAs, timely notification of breaches and appointing a DPO are very much similar to the obligations put on the data controllers under GDPR
6. Penalties fines of 2 per cent or 4 per cent of the global turnover proposed are similar to fines proposed under GDPR.

Beside these similarities with GDPR, the bill proposes developments which suggest that applicability in the Indian market has been kept in mind while drafting it. Some of the developments include (but not limited to):

1. Clearer legal grounds of processing identified for treating personal data related to employment, which was not very explicit under GDPR
2. Annual data audits by independent data auditors mandated for the data fiduciaries. Adoption of an established assurance programme and certification is likely to ensure that organisations adhere to this requirement
3. Processing for reasonable purposes such as whistleblowing, mergers and acquisitions, credit scoring, etc., have clearly been called out
4. Unlike the role and responsibilities of DPO defined under GDPR, the DPO as per the proposed bill can also simultaneously work in other functions, if necessary. GDPR has defined clear lines of responsibilities for the DPO so as to ensure that no conflicts of interest exist. Lack of similar guidance entrusts the responsibility for avoiding any conflict of interest upon the organisation
5. A clear categorisation of offences performed by various participants (such as private organisations, central or state departments) which will fall under the proposed bill has been provided. Further, a layered and descriptive penalty structure, for non-compliance is introduced
6. Exemptions to the obligations proposed under the bill including the processing of personal data for security of state, for journalistic purposes, domestic purposes have been clearly laid out.



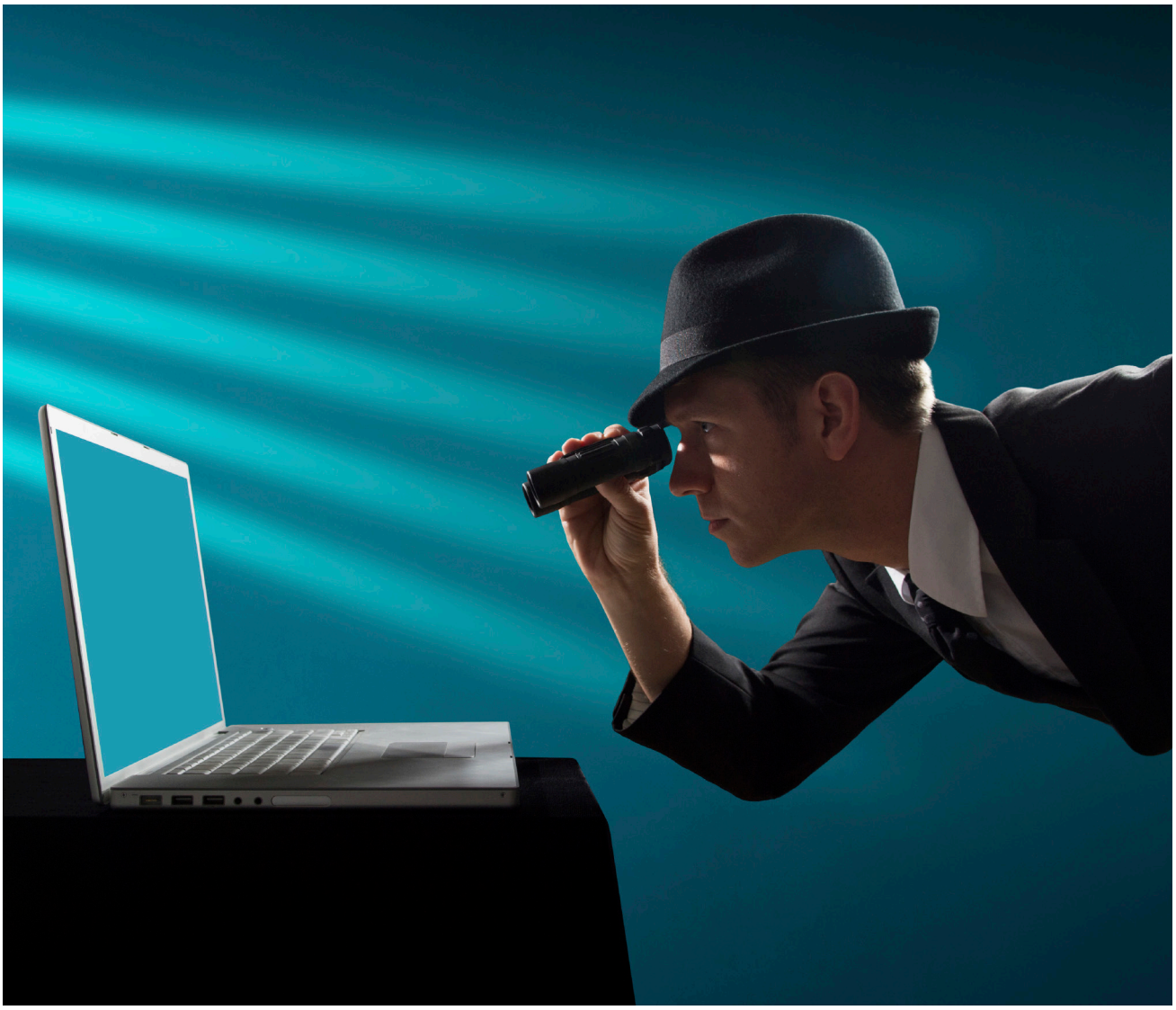
Way forward

With the world becoming more and more sensitive towards the privacy of individuals, the enactment of PDPB is expected to strengthen India's stature as a 'safe country' to handle and process personal data. The successful implementation of PDPB is likely to lay a foundation of data privacy in India and drive a culture shift in how personal data is perceived, processed and protected by organisations across the country. It will also help ensure that India continues its ascension in the digital economy and develops into a lucrative destination for data driven companies across the world.

The regulatory bodies, law enforcement and judiciary would also have to be equipped, trained and undergo capacity building to regulate and enforce the provisions of the PDPB to ensure that the rights are protected while avoiding a situation of creating frivolous grounds by individuals to roadblock efficient functioning of administration, executive and judiciary.

Private sector organisations will be required to take a stock of the personal data they hold and upskill their staff to perform the business transformation required to meet the obligations set out by this bill. Although organisations are to be provided 12 months for transitioning after PDPB's enactment to ensure compliance, the period is seemingly low based on the lessons learnt from implementation of regulations such as GDPR. It is essential that data protection is taken up as a key boardroom agenda to drive organisation wide compliance to prevent the management from becoming liable for various non-compliances and heavy criminal and financial implications.

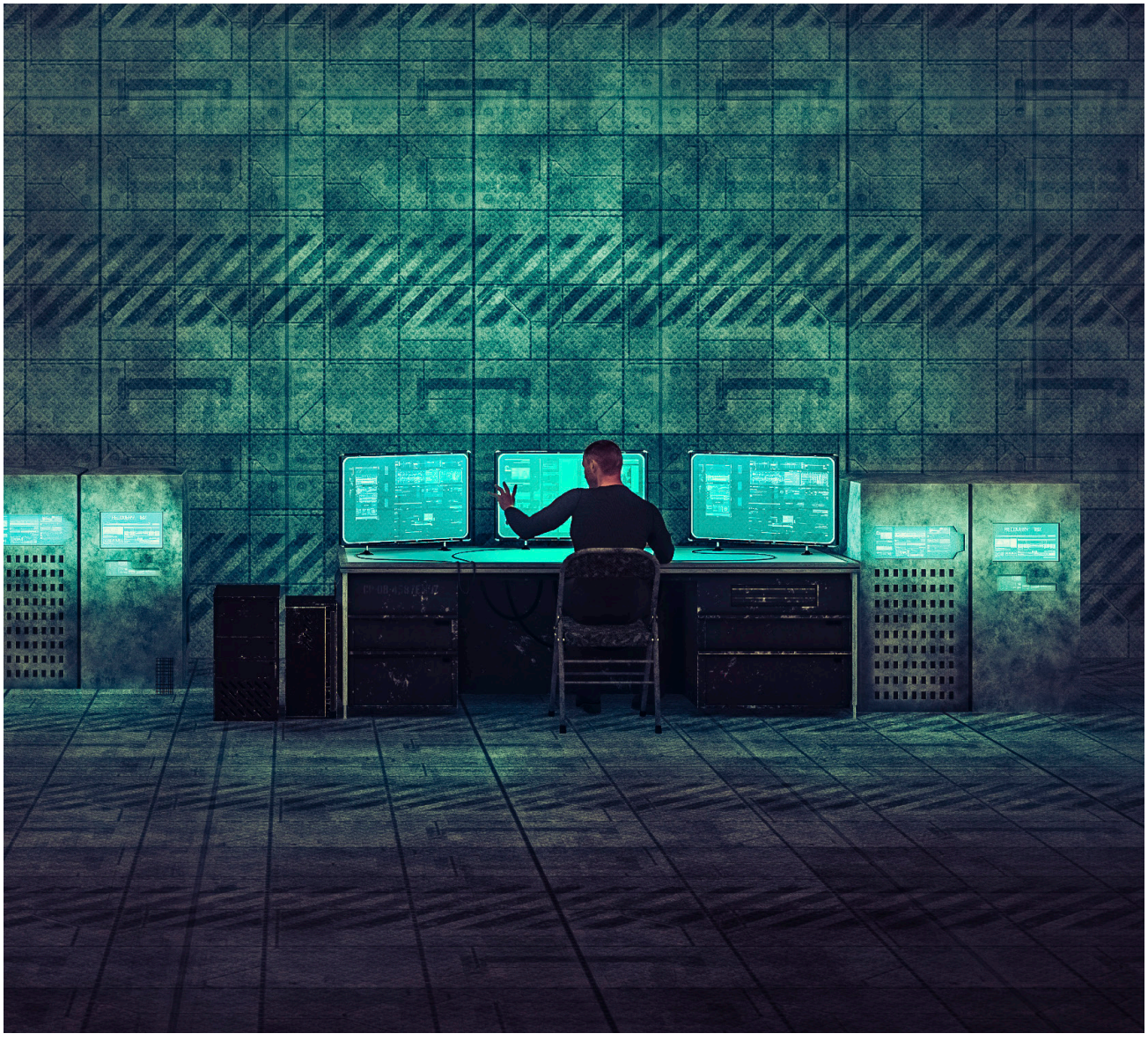
To lead the new privacy regime, it is time various organisations use this opportunity to rethink their obligations and find new, relevant ways to fulfil their fiduciary obligations and restore data principals' trust in their ability to collect, process, handle and disseminate personal data.



Appendix

Legend box

Abbreviation	Description
CBI	Central Bureau of Investigation
DF	Data Fiduciary
DPAI	Data Protection Authority of India
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
GDPR	General Data Protection Regulation
PDPB/ the Bill	Personal Data Protection Bill, 2018
SC	Honorable Supreme Court of India
SDF	Significant Data Fiduciaries
The Committee	The Justice Srikrishna Committee
UIDAI	Unique Identification Authority of India
UOI	Union of India



History of privacy rights in India

Citation	Timeline	Event/milestone
1954 SCR 1077	1954	The right to privacy is not protected by the Indian Constitution – SC in MP Sharma v. Satish Chandra, District Magistrate, Delhi
1964 SCR (1) 332	1962	The right to privacy is not protected by the Indian Constitution – SC in Kharak Singh v. State of Uttar Pradesh
1978 SCR (2) 621	1978	Horizons of freedom of speech and expression expanded to state that this right is no longer restricted by the territorial boundaries of the country, and that privacy is linked to personal liberty – SC in Maneka Gandhi v UOI
1994 SCC (6) 632	1994	The right to privacy can be both an actionable claim and a fundamental right – SC in R Rajagopal v. State of Tamil Nadu
	1995	The European Data Protection Directive (Directive 95/46/EC) issued to protect individuals regarding processing and free movement of personal data
(1997) 1 SCC 301	1997	The right to privacy extended to communications – interception provisions to be issued only by Home Secretaries and the life of an interception order capped at two months – SC in People's Union for Civil Liberties v. UOI
	2000	India's Information Technology Act, 2000 notified
AIR 2010 SC 1974	2010	Physical privacy and mental privacy differentiated, and a connection of the right to privacy established with Article 20(3) (Right against self-incrimination) – SC in Selvi and others v. State of Karnataka and others
	2011	Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
Special Leave to Appeal (Crl) No (s).2524/2014	2014	Request to use any biometrics without the consent of the person refused for the purposes of investigating a criminal offence – SC in UIDAI & Anr. v. CBI
	2014	The European Parliament adopts GDPR
Special Leave to Appeal (C) No. 804/2017	2016	WhatsApp's new privacy policy of sharing data with Facebook challenged in the Delhi High Court - Karmanya Singh Sareen v. UOI
WRIT PETITION (CIVIL) NO 494 OF 2012	2017	"The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution." – SC in KS Puttaswamy v. UOI. Decisions of the MP Sharma (1954) and Kharak Singh (1962) cases overruled to the extent they held that the Indian Constitution did not protect the right to privacy
RBI/2017-18/153 DPSS.CO.OD No. 2785/06.08.005/ 2017-2018]	6 April 2018	The RBI circular mandated all system providers to store the data relating to payment systems in India
	25 May 2018	EU GDPR become effective
	27 July 2018	PDPB and the Retired Justice BN Srikrishna Report released

Table of key offences/penalties[2]

PDPB section	Offence	Type of failure/action	Imprisonment/penalty/ compensation
S 70	Failure to comply with data principal requests under Chapter VI	DF fails to comply with any request of the Data Principal that it is entitled to under the PDPB	INR5,000 for each day of default, and fine up to INR1,000,000 in case of SDF, and INR500,000 in other cases
S 71	Failure to furnish report, returns, information, etc.	DF fails to furnish any report, return or information to the DPAI	INR10,000 each day of default, and maximum of INR2,000,000 for SDF and INR500,000 for other cases
S 72	Failure to comply with direction or order issued by DPA	DF or Data Processor fails to comply with any direction or order of the DPAI	For DF – up to INR20,000 each day of default up to INR20,000,000 Data Processor – INR5,000 for each day of default up to INR5,000,000
S 73	Contravention where no separate penalty has been providedt	Where any person fails to comply with any provision of PDPB for which no separate penalty has been provided	Maximum for SDF INR10,000,000, and others INR2,500,000
S 75	Violation of any provision under PDPB	Data principal who suffers harm as a result of any violation of any provision under this bill by a DF or a data processor	Compensation
S 90	Obtaining, transferring or selling of personal data contrary to PDPB	Any person alone or jointly, knowingly or intentionally or recklessly obtains, discloses, transfers, sells or offer to sell **personal data**	Imprisonment up to three years or fine up to INR200,000 or both
S 91	Obtaining, transferring or selling of sensitive personal data contrary to PDPB	Any person alone or jointly with others, knowingly or intentionally or recklessly obtains, discloses, transfers, sells or offers to sell **sensitive personal data**	Imprisonment up to five years or fine up to INR300,000 or both
S 92	Re-identification and processing of de-identified personal data	Any person, knowingly or intentionally or recklessly re-identifies or re-identifies and processes personal data which has been de-identified such personal data without the consent	Imprisonment up to three years or fine of INR200,000 or both
S 95	Offences by companies	Offence committed by a company	Every person who, at the time the offence was committed, was in charge will be deemed to be guilty of the offence
S 96	Offences by Central or State Government departments	Offence committed by any department of the central or state government, or any authority of the state	The Head of the department or authority will be deemed to be guilty of the offence

2. The Personal Data Protection Bill 2018, Government of India, July 2018

Comparison of PDPB with GDPR[3]

Topic	PDPB	EU GDPR
Terminology	Respectively – Data Fiduciary, data processor and data principal	Data controller, data processor and data subject
Data Processing	**Section 4 – Fair and reasonable processing** Data Processor owes a duty to the Data Principal (equivalent to Data Subjects in GDPR) to process such personal data in a fair and reasonable manner	**Chapter 2, Article 5 – Principles relating to processing of personal data** Data controllers (equivalent to Data Fiduciaries in PDPB) must provide transparent information to Data Subjects when the personal data is obtained
Data Breach Notification	**Section 32 – Personal data breach** a. Data Fiduciary shall notify the DPAI of any personal data breach relating to any personal data processed by Data Fiduciary within the time period specified by the DPAI b. DPAI shall determine if such breach should be reported to the Data Principal	**Chapter 4, Section 2, Article 33** a. Notification within 72 hours of breach of a personal data to the Supervisory Authority is mandatory b. Data processors shall notify their customers, the controllers, 'without undue delay' after first becoming aware of a data breach
Consent	**Section 12 - Processing of personal data on basis of consent** a. Personal Data may be processed with consent of the Data Principal, given no later than at the commencement of processing b. For the consent to be valid, it must be free, informed, specific, clear and capable of being withdrawn	**Chapter 2,Article 7: Conditions for consent** a. The conditions for consent have been strengthened, as the request for consent must be given in an intelligible and easily accessible form b. Consent must be clear and distinguishable from other matters and capable of being withdrawn
Right to Access	**Section 24. Right to confirmation and access by the data principal** Data Principal's rights to obtain from Data Fiduciary: a. Confirmation whether the Data Fiduciary is processing or has processed personal data b. A brief summary of what personal data being processed or has been processed c. A brief summary of processing activities undertaken by Data Fiduciary regarding the personal data	**Section 2, Article 15: Right of access by the data subject** a. The right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose b. The controller shall provide a copy of the personal data, free of charge, in an electronic format

3. European Parliament, Council of the European Union, April 2016; The Personal Data Protection Bill 2018, Government of India, July 2018

Topic	PDPB	EU GDPR
Right to be Forgotten	**Section 27: Right to be forgotten** The Data Principal's right to restrict or prevent continuing disclosure of personal data by a Data Fiduciary where the disclosure – a. Has served the purpose for which it was made or is no longer necessary b. Was made on the basis of consent under Section 12 and such consent has since been withdrawn c. Was made contrary to the provision of PDPB or any other law	**Section 3, Article 17: Right to erasure** a. Entitles the data subject to make Data controller erase his/her personal data, cease further dissemination of the data, and halt processing of the data by third parties b. The conditions for erasure are that data no longer being relevant to original purposes for processing, or a data subject withdraws consent
Data Portability	**Section 26: Right to data portability** The Data Principal shall have the right to receive the personal data in a structured, **commonly used and machine-readable format.**	**Chapter 3,Section 3, Article 20: Right to data portability** Data Subject can receive the personal data which it previously provided in a **commonly used and machine readable format** and has the right to transmit it to another controller
Extra-territorial applicability	**Section 40: Restrictions on cross-border transfer of personal data** a. Data Fiduciary to ensure that storage, on a server or data centre located in India, of at least one serving copy of personal data b. The central government to notify categories of personal data as critical personal data which shall only be processed in a server or data centre located in India	**Article 3: Territorial scope** GDPR applicable to all organisations processing the personal data of data subjects residing in the European Union, regardless of the organisations' location
Right to Compensation	**Section 75: Compensation** a. Any Data Principal who suffers harm due to violation by a Data Fiduciary or a Data Processor, will have the right to seek compensation b. Data Processor will be liable if it: i. acted outside or contrary to the instructions of the Data Fiduciary for processing ii. acted in a negligent manner iii. has not incorporated adequate security safeguards iv. violated any provisions expressly applicable to it	**Section 82: Right to compensation and liability** a. Any person who has suffered material or non-material damage has the right to receive compensation from the controller or processor b. Any controller involved in processing is liable for the damage caused by processing. A processor to be liable for the damage caused by processing only where it has not complied with obligations of GDPR specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller

KPMG in India contacts:

Nilaya Varma
Partner and Leader
Markets Enablement
T: +911246691000
E: nilaya@kpmg.com

Atul Gupta
Partner and Head
IT Advisory - Risk Consulting
Cyber Security Lead
T: +91 124 307 4134
E: atulgupta@kpmg.com

Maneesha Garg
Partner and Co-Head
Forensic Services
Lead - Corporate Intelligence
T: +91 120 386 8501
E: maneesha@kpmg.com

Ravindranath Patil
Director
Forensic Services
T: +91 206 747 7017
E: ravindranathpatil@kpmg.com

Akhilesh Tuteja
Partner and Head
Risk Consulting
Co-Leader - Global Cyber Security
T: +91 124 336 9400
E: atuteja@kpmg.com

Jagvinder S Brar
Partner and Co- Head
Forensic Services
T: +91 123 336 9469
E: jsbrar@kpmg.com

Mayuran Palanisamy
Director
IT Advisory - Risk Consulting
Data Privacy Lead
T: +91 44 39145218
E: mpalanisamy@kpmg.com

#KPMG josh

Follow us on:
home.kpmg/in/social media