DATA PROTECTION BILL, 2019

The Data Protection Bill, 2019 ("Bill") has been proposed to protect the sanctity of data belonging to natural persons and for setting up an Authority for ensuring the fundamental right of privacy and protection of personal data of the citizens of India. Through this article, we would attempt to understand the Bill and the changes that will come into force once the Bill is enacted. We are evaluating the said topic to gain a brief insight of the Bill through this article.

Existing Legal Framework

At present the Personal Data of individuals is protected by Section 43-A of the Information and Technology Act, 2000 and Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. Once the Bill is enacted into an Act, this Section shall be omitted. The existing framework is a consent-based regime and provides for compensation in case of unauthorized access to or disclosure of sensitive personal data, however, with the enactment of the Bill into an Act, the framework would shift to a more regulated regime with severe penal consequences.

Background

In the matter of Justice K.S. Puttaswami and another Vs. Union of India [WP 494 of 2012], "privacy" was declared a fundamental right under Article 21 of the Constitution. While, delivering the Judgement, the SC emphasized that the Government needed to bring out a robust data protection regime.

In order to act on the recommendations of the SC and address the issues surrounding the subject, the Government on 31st July 2017 constituted a "Committee of Experts on Data Protection". Based on the report of the Committee and suggestions received from the stakeholders, the Bill was laid out.

Definitions under the Bill

The Bill has provided the following definitions:

i. "*Personal Data"* shall include:
   a. Data about or relating to a natural person;
   b. Such data would be with regard to:
      - any characteristic,
      - trait,
      - attribute
      - any other feature of the identity of such natural person,
      - any combination of such features with any other information;
   c. Such data may be directly or indirectly identifiable to such natural person;
   d. Such data shall include any inference drawn from the above-mentioned data for the purpose of profiling.

ii. "*Data Principal*" has been defined as the natural person to whom such *Personal Data* relates to.

iii. "*Data Fiduciary*" has been defined as any person who alone or in conjunction with others determines the purpose and means of processing of *Personal Data*.

iv. "*Data Processor*" has been defined as any person who processes data on behalf of a *Data Fiduciary*. It is clear from the definition of *Data Fiduciary* and *Data Processor*, the term "person" mentioned therein, would include the State, a company, any juristic entity or any individual.

v. "*Processing"* has been defined as an operation or set of operations performed on *Personal Data*, including operations such as:

- collection,
- recording,
- organizing,
- structuring,
- storage,
- adaptation,
- alteration,
- retrieval,
- use,
- alignment or combination,
- indexing,
- disclosure by transmission,
- dissemination or otherwise making available,
- restriction,
- erasure, or
- destruction.

vi. "*Sensitive Personal Data*" means such *Personal Data*, which may, reveal, be related to, or constitute—

- 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; or
- any other data categorised as Sensitive Personal Data by the Government in consultation with the Data Protection Authority and sectoral regulator.

Applicability of the Bill

The Bill shall be applicable to the following:

Applicability of the Bill	i. Territorial: a. Processing of Personal Data: in cases where Personal Data processed by way of collection, disclosure, sharing or otherwise, *within the territory of India*; b. Personal data processed for State, any Indian company, any citizen of India or any person or body of persons incorporated or created under Indian law.
	ii. Extra-territorial: Data Fiduciaries or Data Processors outside the territory the territory of India shall fall under the ambit of the Bill, if personal data being processed by them is— a. in connection with any business carried on in India, or b. any systematic activity of offering goods or services to Data Principals within the territory of India; or c. in connection with any activity which involves profiling of Data Principals within the territory of India.

The Bill shall not be applicable to the processing of anonymised data, other than any personal data anonymised or other non-personal data sought by the Central Government to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government.

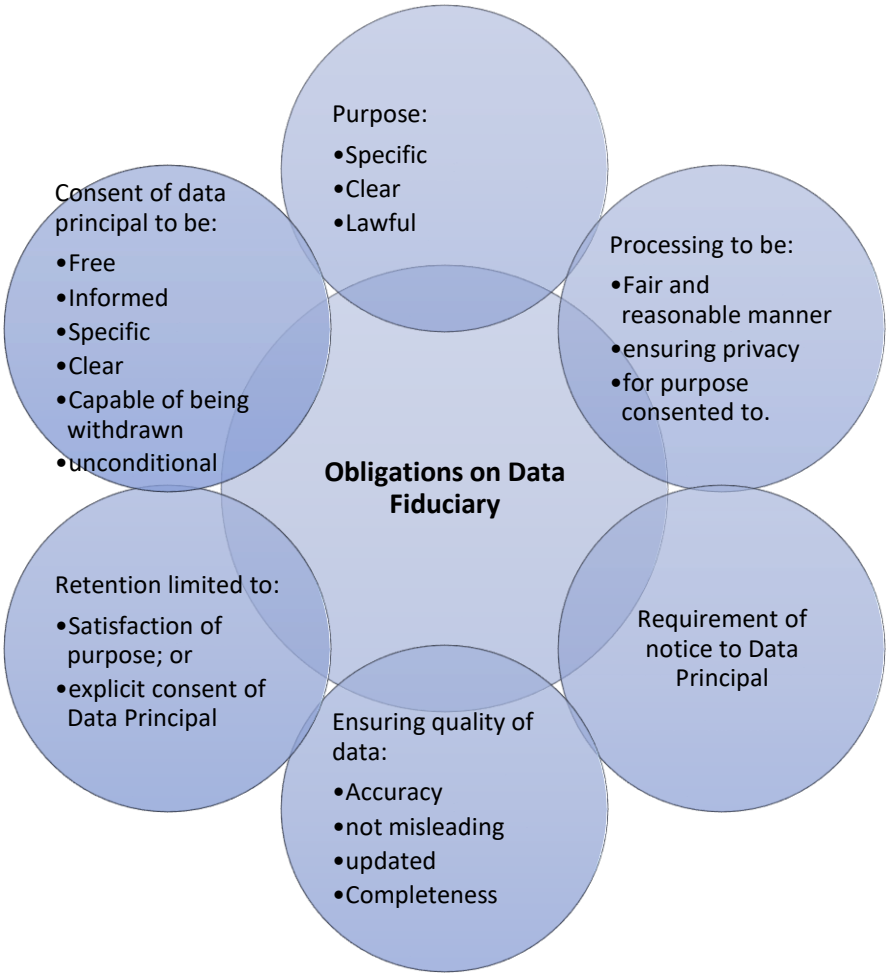
Provisions of the Bill

The Bill has specified the following Chapters in the Bill, of which a few will be discussed in our article:

1. Obligations of Data Fiduciaries
2. Grounds for processing of Personal data without consent
3. Personal Data and Sensitive Personal Data of Children
4. Rights of Data Principal
5. Transparency and Accountability
6. Restriction on Transfer of Personal Data
7. Exemptions
8. Offences and penalties

1. Obligations of Data Fiduciary

The Bill imposes the following obligations on a Data Fiduciary:



2. Grounds for processing of Personal Data without consent

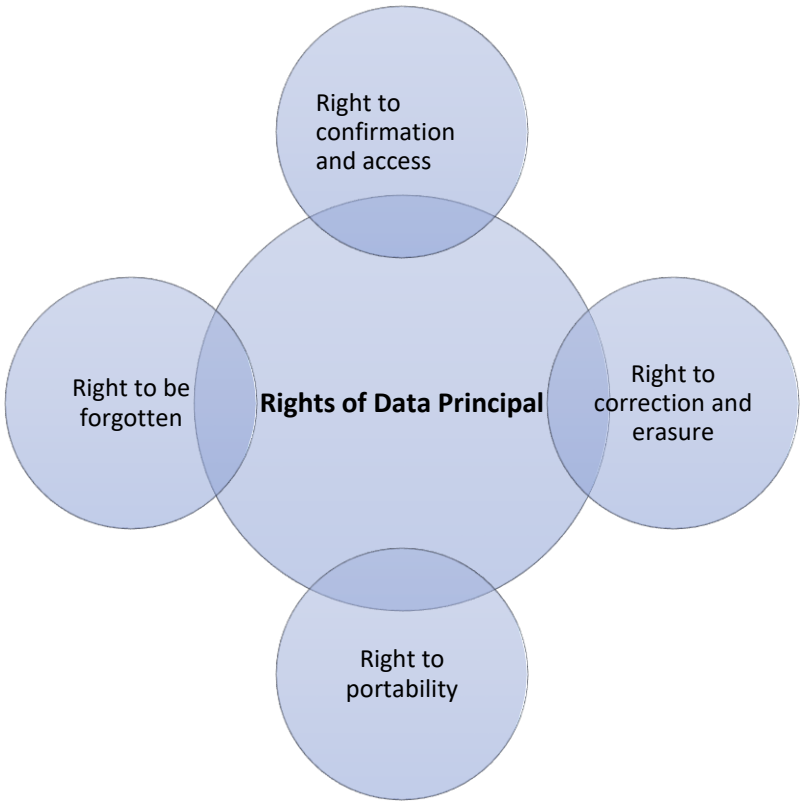
Grounds for processing of Personal Data without consent	- Under Law in force
	- Compliance with any Order or Judgment of any Court of Tribunal
	- In response to any medical emergency
	- Medical treatment during epidemic, outbreak or any threat to public health
	- Ensuring safety during any disaster or breakdown of public order
	- Performance of State function
	- Necessary for recruitment, termination, service benefit to employee, assesment of performance. Sensitive Personal Data may not be processed under this provision.
	- For other purposes as may be specified by Data Protection Authority

3. Personal Data and Sensitive Personal Data of Children

The Bill provides the following:

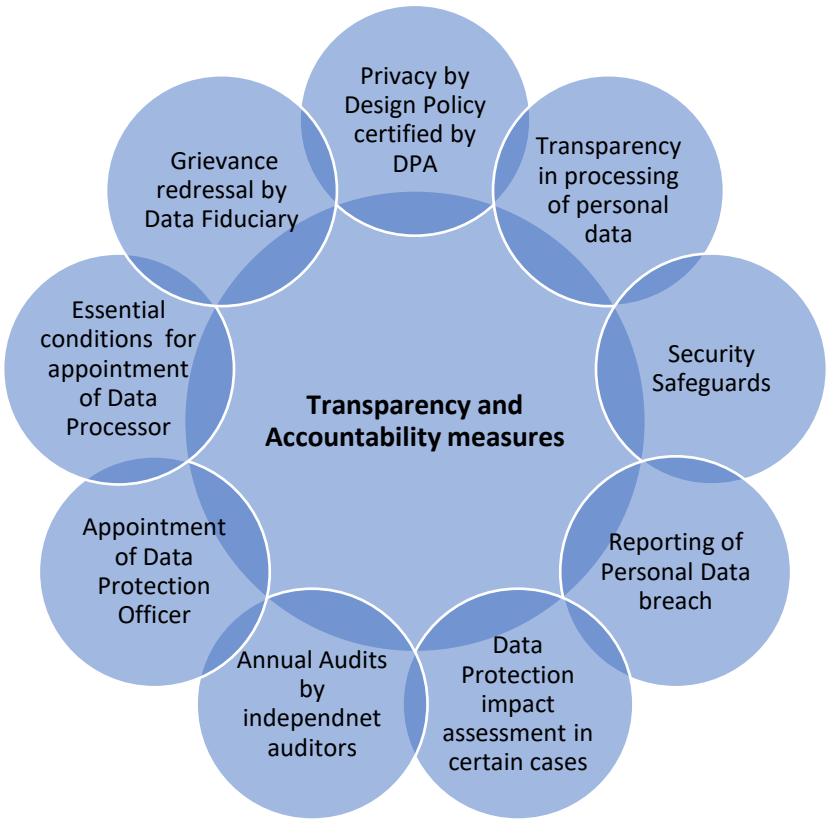
- Compliances before processing Personal Data of a child: An obligation to verify the age of a child and obtain consent from a parent or guardian of such child.
- Classification as "Guardian Data Fiduciary": The Data Protection Authority may classify a Data Fiduciary as "Guardian Data Fiduciary", if such Data Fiduciary provides website or online services directed at children or process large volumes of personal data of children.
- Guardian Data Fiduciary has been barred from profiling, tracking or behaviorally monitoring of, or targeted advertising directed at, children and undertaking any other processing of personal data that can cause significant harm to the child.
- Guardian Data Fiduciary providing exclusive counselling or child protection services to a child shall be exempted from seeking consent from guardian or parent of Data Principal who is a child.

4. Rights of Data Principal



5. Transparency and Accountability Measures

The following measures have been prescribed for Data Fiduciaries:



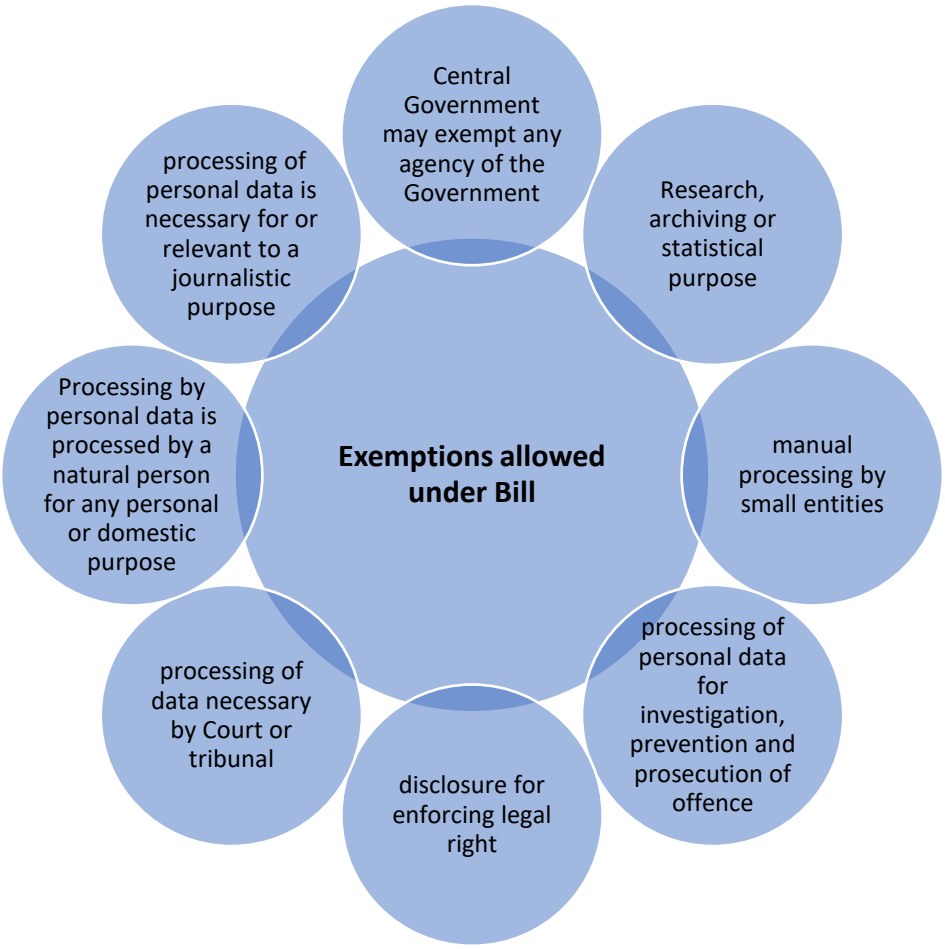
6. Restriction on transfer of data

The Bill provides that a notice to the Data Principal should be given regarding transfer of data outside India, at the time of collection of such data.

Scope	Personal Data	Sensitive Personal Data	Critical Personal Data
Consent Requirement	Consent at the time of collection for processing	Explicit Consent and approval of DPA	Not permissible
Conditions of transfer	Not prescribed	One copy to be maintained in India	Transfer may be allowed if: a. necessary for prompt action pursuant to an emergency and the receiving party is in health or emergency service. b. if transfer permissible by DPA and Central government.

7. Exemptions under the Bill

The Bill provides for the following exemptions:



8. Penalties

The Penalties prescribed under the Bill are as follows:

Offence	Penalty and/ or imprisonment	Liable entity
• Processing of personal data in violation of provisions. • Processing of personal data of child in violation of provisions • Transfer of data outside India in violation of provisions	Higher of up to INR 15 Crore or 4 per cent of worldwide turnover of preceding financial year	Data Fiduciary

• Failure to take appropriate action in case of data breach • Failure to register with DPA • Failure to take data protection impact assessment by significant data fiduciary	Higher of up to INR 5 Crore or 2 per cent of worldwide turnover of preceding financial year	Data Fiduciary
• Failure to comply with direction or order of DPA	Data Fiduciary- up to INR 20,000 per day of default, subject to maximum of INR 20 Crore Data Processor- up to INR 5,000 per day of default, subject to maximum of INR 50 Lakh	Data Fiduciary/ Data Processor
• Person who re-identifies, de-identified personal data	Imprisonment not exceeding 3 years or fine up to INR 2 lakh rupees or both	Any person

Conclusion

With the introduction of this Bill, India has shown its intention to treat the personal data of its individuals with higher reverence and in accordance with global standards. Once this Bill is passed, we can expect a significant decrease in crimes related to identity thefts.

Organizations would need to incorporate several changes in their structure at every level to comply with the provisions of the Bill.

This article is also published in Taxguru : https://taxguru.in/corporate-law/data-protection-bill-2019.html