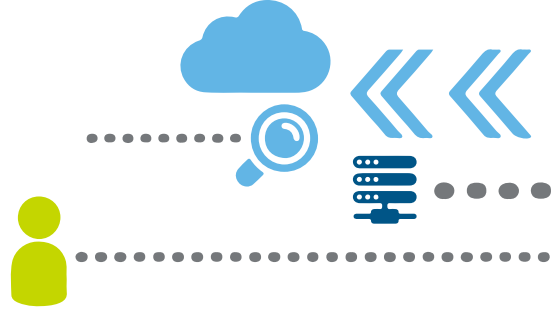
Deloitte.

Draft Personal Data Protection Bill, 2019

Private and confidential
January 2020

Risk Advisory

Existing privacy laws



Privacy under IT Act 2000

In the absence of a specific law on privacy, the right to privacy is legally viewed under the Information Technology (IT) Act, 2000. The Act has some express provision guarding individuals against breach of privacy by corporate entities.

SPDI* Rules

Exercising its powers under Section 43A of the IT Act 2000, the government notified SPDI rules to protect privacy of an individual. These all relate to seeking permission by a company before accessing privacy data of individuals and fixing liabilities for violation of the same.

Privacy as a fundamental right

Beyond this, the right to privacy is dealt with under Article 21 of the Constitution. The Supreme Court in Puttaswamy judgement linked the right to privacy as part of the right to life and personal liberty guaranteed under Article 21.

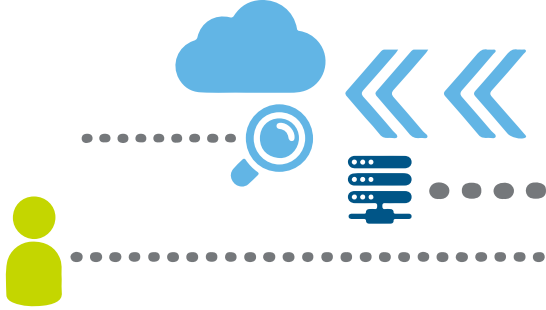
*The Information Technology (Reasonable Security Practices and Procedures and **Sensitive Personal Data or Information**) **Rules 2011**

Reference: http://www.dot.gov.in/sites/default/files/itbill2000_0.pdf

Reference: http://www.supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf

Executive summary

Personal Data Protection Bill, 2019



The Personal Data Protection Bill, 2019 released on 10 December 2019 introduced key changes from its draft version which was released last year on 27 July 2018 (referred to as PDPB 2018). Post approval by the Union Cabinet, the India Personal Data Protection Bill, 2019 (PDPB 2019) was introduced in the Lok Sabha (Parliament) by the Minister of Electronics and Information Technology, Mr. Ravi Shankar Prasad, on December 11, 2019.

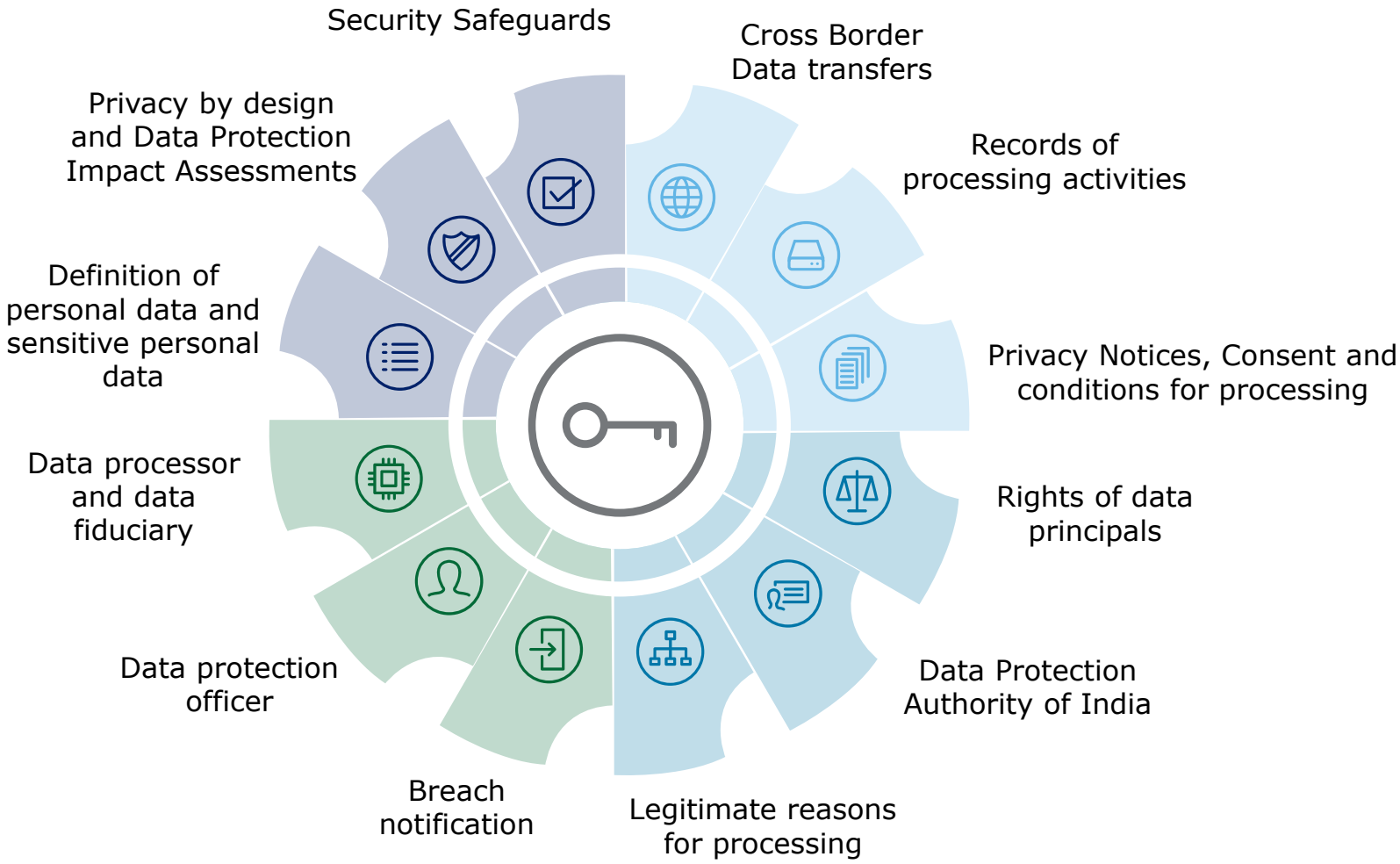
Applicability: The Bill governs the processing of personal data by:

- government
- companies incorporated in India, and
- foreign companies dealing with personal data of individuals in India.

The Bill seeks to provide for protection of personal data of individuals, and establishes a Data Protection Authority for the same. It was decided to refer the Bill to a Parliamentary Select Committee for review. Post this review the India PDPB 2019 will be introduced in the Budget session (tentatively in first week of Feb 2020).

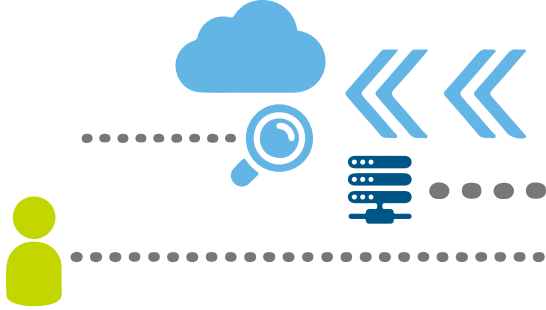
Protection of personal data of data principal is at the core of draft Personal Data Protection Bill, 2019 (hereafter referred as "PDPB" or "bill"). This means once the bill is enacted and enforced, privacy will no longer be an option and cannot be ignored. Among many significant provisions, the PDPB proposes substantial penalty for violation of the stated requirement. Such provisions, along with heightened focus on collection and use of personal data, will require organizations (referred in the bill as Data fiduciary and Data processor) to revisit their risk acceptance criteria and establish a robust privacy and data protection framework.

Key requirements of PDPB 2019



Key roles and definitions

Personal Data Protection Bill, 2019



Data Principal

Data principal means the natural person to whom the personal data relates

Data Fiduciary

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

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;

Personal data

Personal data means 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, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling

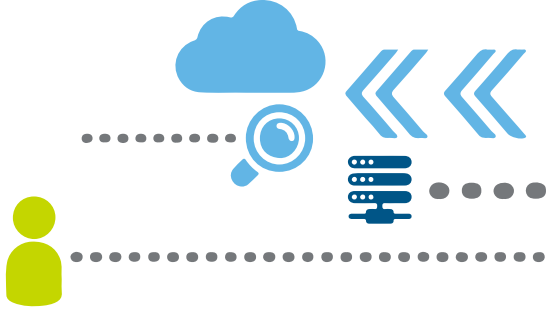
Sensitive Personal data

Sensitive personal data means such personal data, which may, reveal, be related to, or constitute—

- Financial Data
- Health Data
- Sex life
- Sexual Orientation
- Biometric Data
- Official Identifier
- Genetic Data
- Transgender Status
- Intersex Status
- Religious political belief or affiliation
- Any other data categorized as sensitive personal data under section 15
- Caste or tribe

Implications

The bill proposes two tier system to assess violation(s) and impose penalty as per Chapter X - Penalties and Compensation



Obligations, if violated may lead to penalty

1. Prompt and appropriate action in response to a data security breach
2. Failure to register with the Authority
3. Undertaking a data protection impact assessment by a significant data fiduciary
4. Conducting a data audit by a significant data fiduciary
5. Appointment of a data protection officer by a significant data fiduciary

INR 5Cr* Or **2%**
of global turnover, whichever is higher

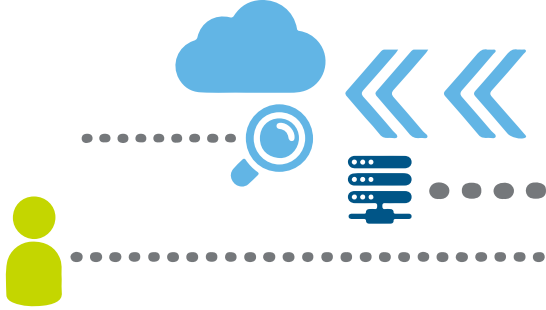
Obligations, if violated may lead to penalty

1. Ground of processing of personal data
2. Ground of processing of sensitive personal data
3. Ground of processing of personal and sensitive personal data of children
4. Adhering to data security safeguards
5. Transfer of personal data outside India subject to defined conditions

INR 15Cr* Or **4%**
of global turnover, whichever is higher

*where of any provisions has been contravened by the State, the maximum penalty shall not exceed five crore rupees under sub-section (1), and fifteen crore rupees under sub-section (2), respectively

Key changes from PDPB 2018



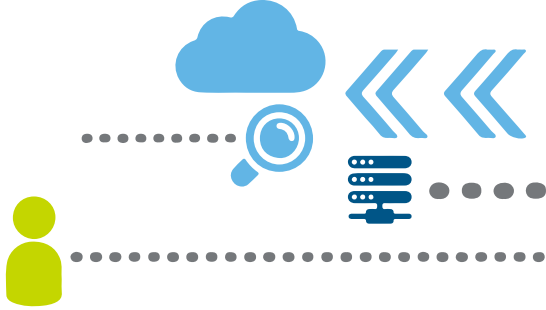
The Personal Data Protection Bill, 2019, has three broad differences from its draft version which are the :

1. **Changes to select provisions**
2. **Insertions of additional requirements and**
3. **Deletions from the earlier version of the bill.**

Below are the changes to select provisions

Art. No. (PDPB 2019)	Change from PDPB 2018	Description of change
17	**Added constraint to Right to Confirmation and Access**	The data principal shall have the right to access in one place the identities of the data fiduciaries with whom his personal data has been shared by any data fiduciary together with the categories of personal data shared with them, in such manner as may be specified by regulations.
3	**Change in definition of personal data**	"Personal data" means data relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic or any other feature of the identity of such natural person, whether online or offline, and shall include any inference drawn from such data for the purpose of profiling
34	**Cross border data transfer for sensitive personal data**	There is no restriction on transfer of personal data outside India, however, sensitive personal data may only be transferred for processing outside India with the user's explicit consent and the Data Protection Authority's ("DPA") or Central government's permission, but can only be stored in India.
18	**Added constraint to Right to Correction**	The erasure of personal data which is no longer necessary for the purpose for which it was processed.
3	**Change in definition of sensitive personal data**	Passwords" have been removed from the list of sensitive personal data elements in the PDPB 2019.

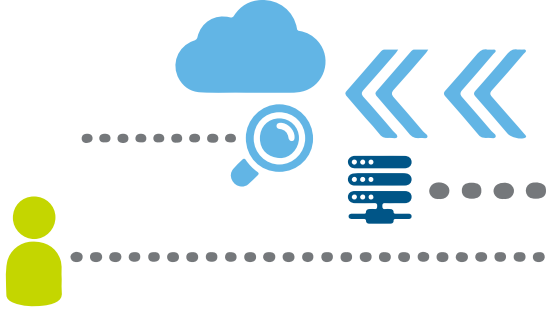
India Personal Data Protection Bill, 2019 – New insertions



Below are the Insertions of additional requirements

Art. No.	Topic	Details
3	**Definitions**	A **Consent manager** is defined as a data fiduciary which enables a data principal to gain, withdraw, review, and manager his consent through an accessible, transparent, and interoperable platform; **"In writing"** Includes any communication in electronic format as defined in clause (r) of sub-section (1) of section 2 of the Information Technology Act, 2000; **Data auditor** means an independent data auditor and **"Regulations"** means the regulations made by the Authority under this Act
22	**Privacy By Design Policy**	Every data fiduciary shall **prepare a privacy by design policy**; Subject to the regulations made by the Authority, the data fiduciary may submit its privacy by design policy prepared under pt. (1) to the Authority for certification within such period and in such manner as may be specified by regulations; The Authority, or an officer authorized by it, shall certify the privacy by design policy on being satisfied that it complies with the requirements pt. (1); The privacy by design policy certified under sub-section (3) shall be published on the website of the data fiduciary and the Authority.
	Social Media Intermediary	***Social media with a certain high volume of users and ability to impact electoral democracy***, India's security, sovereignty or public order, can be notified by the Central government and DPA as a ***significant data fiduciary*** (Entities processing high volumes of sensitive data).
40	**Sandbox**	The Authority shall, for the purposes of encouraging innovation in artificial intelligence, machine-learning or any other emerging technology in public interest, create a Sandbox.

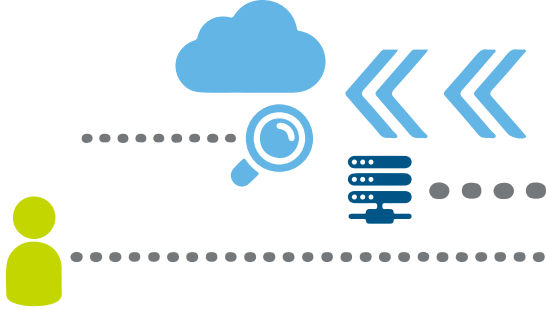
India Personal Data Protection Bill, 2019 – New insertions



Below are the Insertions of additional requirements

Art. No.	Topic	Details
28	**Verification**	Social media intermediaries classified as significant data fiduciaries will now have to give **account verification options** to willing users. The said verification has to be in the form of a visible mark of verification. The verification process will be voluntary in nature.
91	**Act to promote framing of policies for digital economy etc.**	The 2018 draft provided for power of the Central Government to formulate appropriate policies for the digital economy, including measures for its growth, security, integrity, prevention of misuse, insofar as such policies do not govern personal data. In the 2019 version, **Central Government may, in consultation with the DPA may direct any data fiduciary or data processor to provide any personal data anonymised or other non-personal data to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government.**
	Conditions for transfer of Personal and sensitive personal data	The sensitive personal data may only be transferred outside India for the purpose of processing, when explicit consent is given by the data principal for such transfer, and where— **(a) the transfer is made pursuant to a contract or intra-group scheme approved by the Authority: (b) the Central Government, after consultation with the Authority, has allowed the transfer to a country or, such entity or class of entity in a country or, an international organization (c) the Authority has allowed transfer of any sensitive personal data or class of sensitive personal data necessary for any specific purpose.**
59	**Penalties and Compensation**	where of any provisions referred to in this section has been contravened by the State, the maximum penalty **shall not exceed five crore rupees** under sub-section (1), and fifteen crore rupees under sub-section (2), respectively.

India Personal Data Protection Bill, 2019 – Key deletions

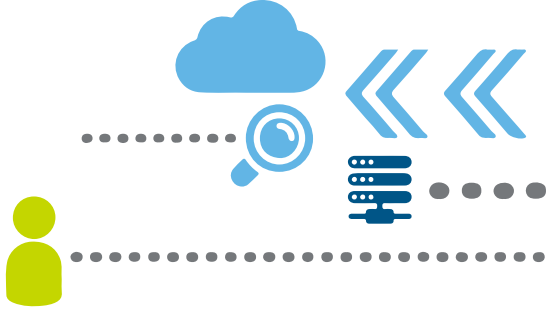


Below are the sections which have been deleted from the Personal Data Protection Bill, 2018 and are not a part of the PDPB 2019

Terms Deleted	Description of terms deleted
Definitions of Harm, Significant Harm and Data Processor from Article 3	**"Harm "** includes— (i) bodily or mental injury; (ii) loss, distortion or theft of identity; (iii) financial loss or loss of property, (iv) loss of reputation, or humiliation; (v) loss of employment; (vi) any discriminatory treatment; (vii) any subjection to blackmail or extortion; (viii) any denial or withdrawal of a service, benefit or good resulting from an evaluative decision about the data principal; (ix) any restriction placed or suffered directly or indirectly on speech, movement or any other action arising out of a fear of being observed or surveilled; (x) any observation or surveillance that is not reasonably expected by the data principal. **"Significant harm "** means harm that has an aggravated effect having regard to the nature of the personal data being processed, the impact, continuity, persistence or irreversibility of the harm; **"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*;
Accountability from article 11	Accountability.— (2) **The data fiduciary should be able to demonstrate that any processing undertaken by it or on its behalf is in accordance with the provisions of this Act.**
Every data fiduciary shall **ensure the storage, on a server or data center located in India,** of at least one serving copy of personal data to which this Act applies. (Article 40)	The 2019 version of PDPB has put an **end on the blanket data localization**. The necessity of storing at **least one serving copy** in a data center located in India has been done away with.

* Text in bold has been removed from this year's definition

Concluding remarks



The Personal Data Protection Bill seeks to lay down a lawful framework to reserve the inviolability of " consent " in data transfer and processing and also proposed to penalize those breaching the privacy norms. It allows processing of individual's data only for lawful purposes.

The bill compels data fiduciaries to start processing data in India. Due to such high level of data consumption, it is expected that India is likely to become one the biggest centers of data refinery in the coming years.

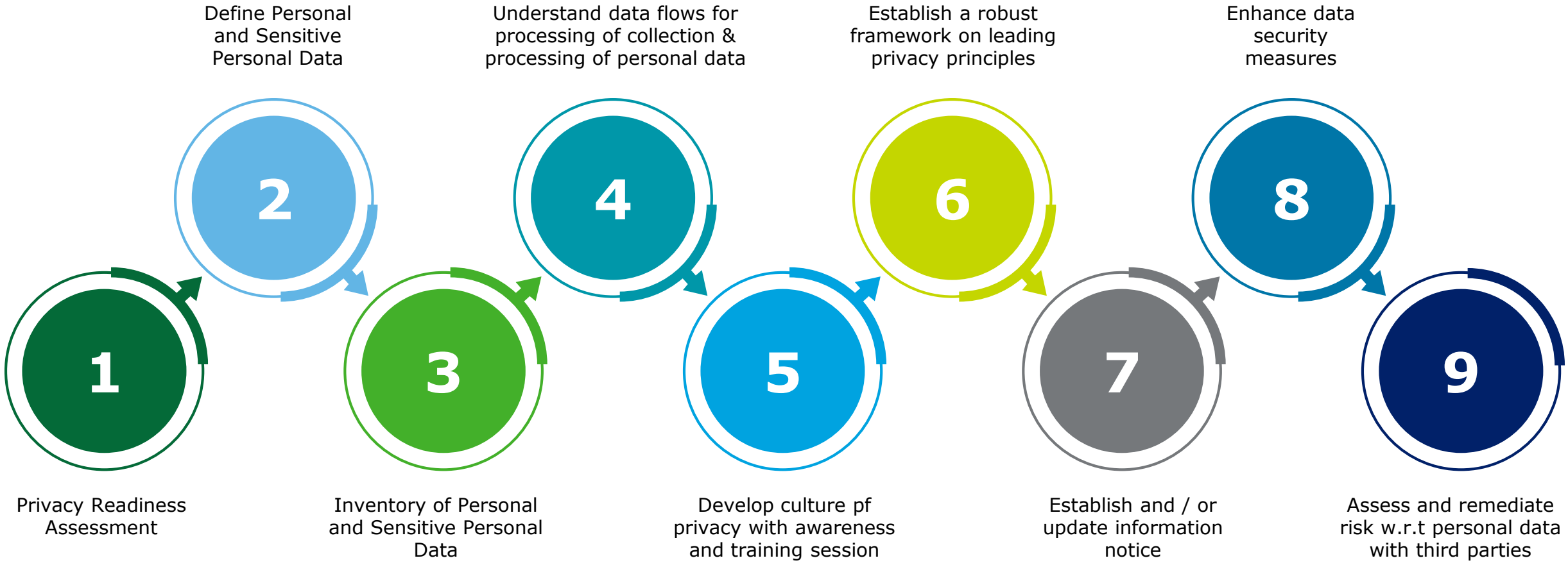
Given that India doesn't have a pre defined framework which insures protection of an individual's data, the introduced bill is essential. Its expected that PBPB will ensures confidentiality across sectors and wont limit to a particular sector

The robust framework is likely to promote 'privacy, the fundamental right for data principal', enhance India's data sovereignty status because of proposed limitations sensitive personal data outside India

The govt. has segregated the data as sensitive, critical, personal and non personal, as against putting it all in one bucket. This will empower the citizens to have an uninterrupted digital experience while knowing that the data will be collected, used, stored and protected under a strict lawful guideline.

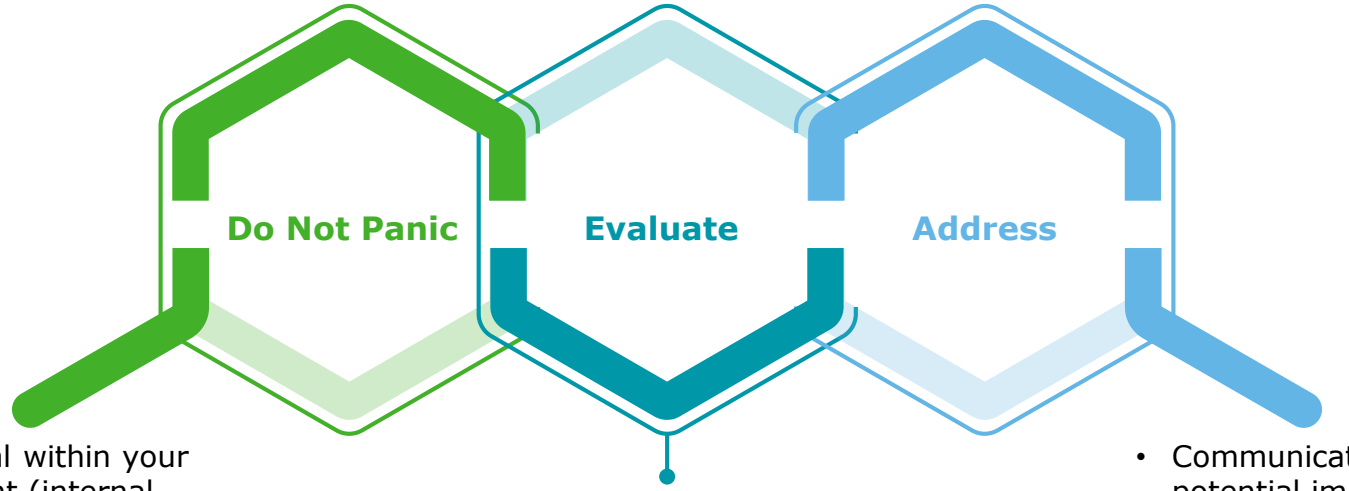
What next? – A proactive approach can help

Until the law gets enacted, organizations may consider following initiatives:



Conclusion

Three step conclusion to address the current situation:

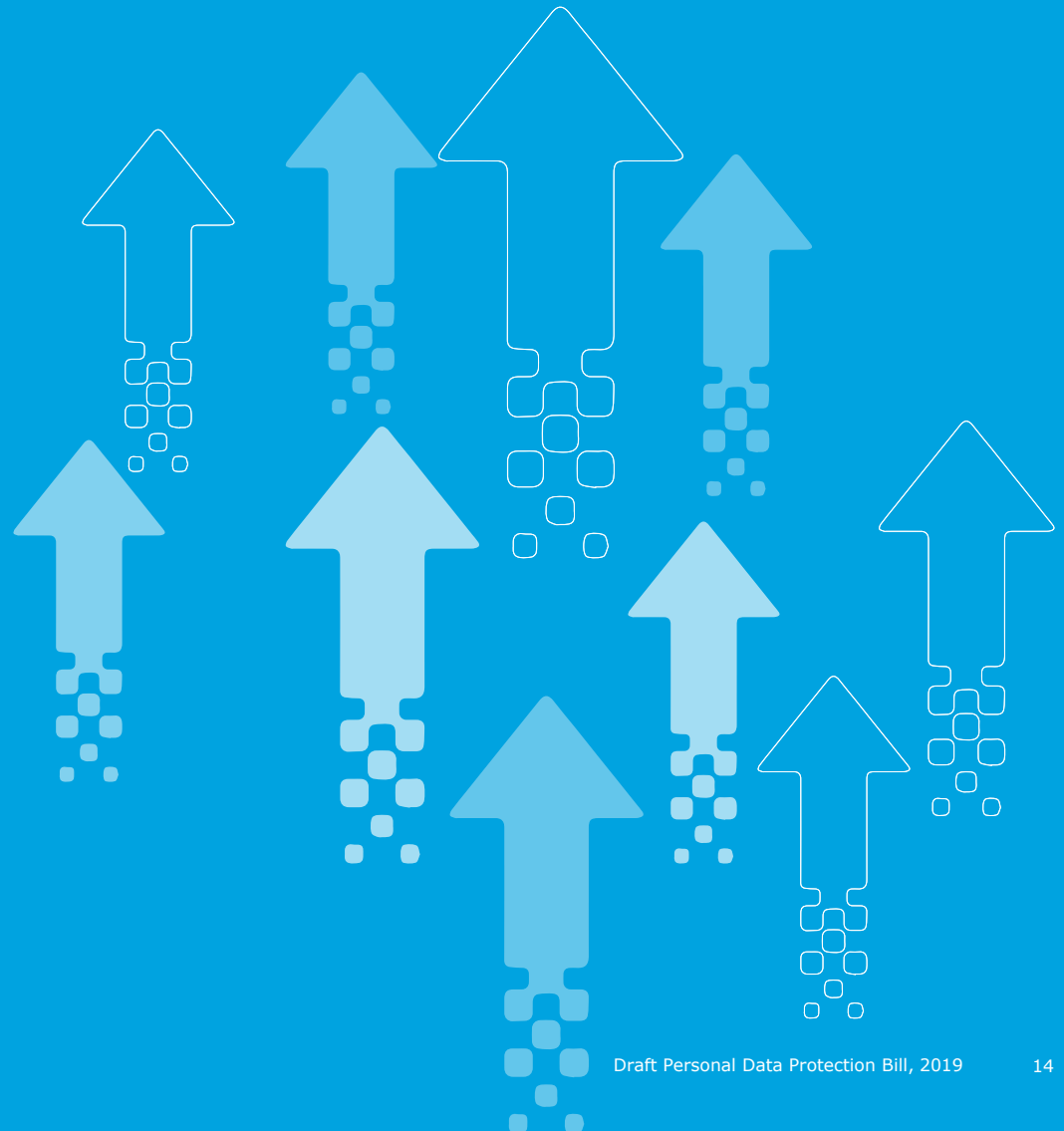


- Identify and empower an individual within your organization to be the contact point (internal, external, regulatory), to monitor, report and plan for changing legal obligations and establish consistent messaging.
- Gather existing documentation on data processing operations, including data transfers, to evaluate risk exposure and prepare for potential inquiries from stakeholders like the Authority (to be established), clients or employees etc.

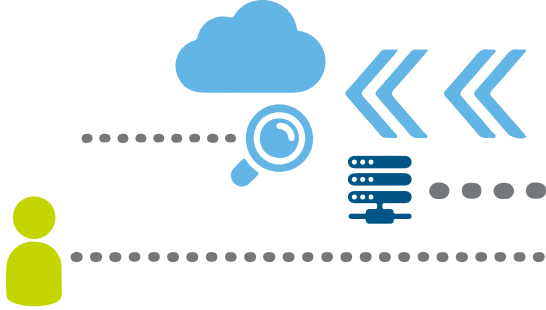
- Develop an inventory of systems, controls, and procedures to understand where personal data are processed and which specific controls (e.g., data usage) exist.
- Assess available cross border transfer methods and shortlist the method(s) that meet the requirements of your organization.
- Assess your current state (e.g., compliance with existing requirements from IT Act 2000, IT Rules 2011 etc. and the draft bill, third party sharing, etc.).

- Communicate regulatory changes and their potential impact to senior stakeholders to raise awareness and obtain senior-level support.
- Develop a risk based remediation strategy and roadmap including a short term tactical plan focusing on “quick wins”.
- Develop and execute a communications plan.

Annexure
A deep dive



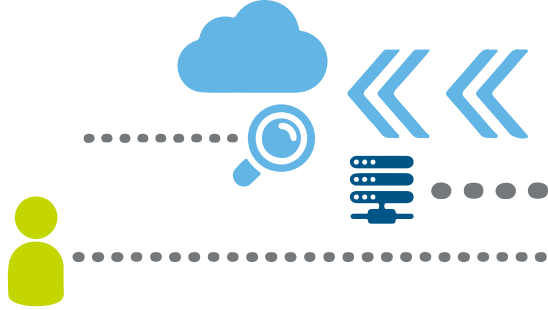
Roles considered under Personal Data Protection Bill, 2019, Enforcement fines and punishments



- **Data principal** means the natural person to whom the personal data relates.
- **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.
- **The Data Protection Authority** will be established by notification by the Central Government and it shall be the duty of the Authority to protection the interests of the data principals by monitoring and enforcing application of the provisions of the Act.
- The Data Protection Officer is responsible to provide information, advise and monitor the processing activities of the data fiduciary to ensure that the provisions of the Bill are not violated.
- The DPO must provide assistance and cooperate with the Authority on matters related to the compliance of the data fiduciary with the provisions of the Bill.
- The DPO must act as a point of contact for the data principal during the grievance redressal procedure under the Bill.
- The data fiduciary can assign any other function to the data protection officer. Based on the type of violation, the administrative fines can extend up to :
  i. *Five crore rupees or two percent of the data fiduciary's total worldwide turnover of the preceding financial year, whichever is higher ; or
  ii. *Fifteen crore rupees or four percent of the data fiduciary's total worldwide turnover of the preceding financial year, whichever is higher
- An offence punishable under this Bill shall be cognizable and non- bailable.

* where of any provisions has been contravened by the State, the maximum penalty shall not exceed five crore rupees under sub-section (*i*), and fifteen crore rupees under sub-section (*ii*), respectively

Defining Personal Data & Sensitive Personal Data



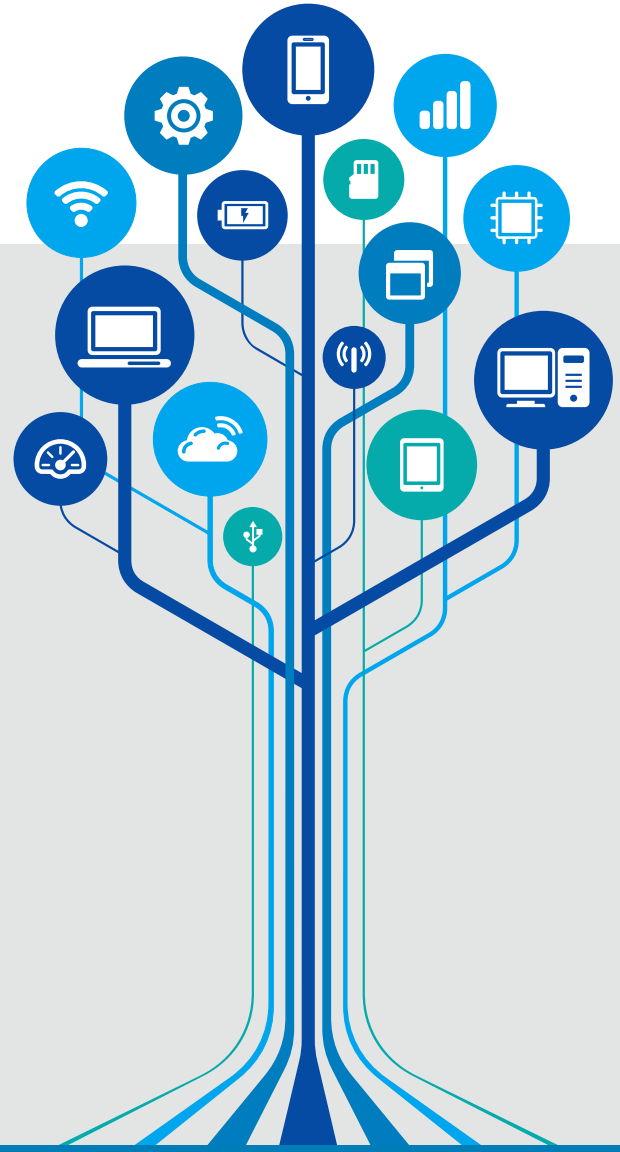
The Personal Data Protection Bill, 2019 defines Personal Data as data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling.

Sensitive Personal Data has been defined to mean personal data which may, reveal, be related to, or constitute

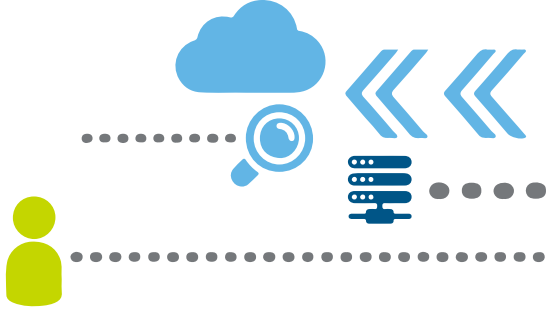
- financial data
- health data
- official identifier
- sex life
- sexual orientation
- biometric data
- genetic data
- transgender status
- intersex status
- caste or tribe
- Religious or political belief or affiliation
- any other category of data specified by the Authority under section 22

Classification of data fiduciaries as significant data fiduciaries

- The Authority shall, having regard to the following factors, notify any data fiduciary or class of data fiduciary as **significant data fiduciary**, namely:—
  1. volume of personal data processed;
  2. sensitivity of personal data processed;
  3. turnover of the data fiduciary;
  4. risk of harm by processing by the data fiduciary;
  5. use of new technologies for processing; and
  6. any other factor causing harm from such processing.
- Every **social media intermediary** which is notified as a significant data fiduciary shall enable the users who register their service from India, or use their services in India, to voluntarily verify their accounts in such manner as may be prescribed.
- Any user who voluntarily verifies his account shall be provided with such demonstrable and visible mark of verification, which shall be visible to all users of the service, in such manner as may be prescribed.
- The notified significant data fiduciaries will need to register with the Authority in the manner that may be specified.
- Any social media intermediary,—
  i. with users above such threshold as may be notified by the Central Government, in consultation with the Authority; and
  ii. whose actions have, or are likely to have a significant impact on electoral democracy, security of the State, public order or the sovereignty and integrity of India, shall be notified by the Central Government, in consultation with the Authority, as a significant data fiduciary



Data protection obligations



01 Processing of data in a free and transparent manner

02 Purposes of processing data must be clear, specific and lawful.

03 Data collected must have a strong nexus with the purpose of processing

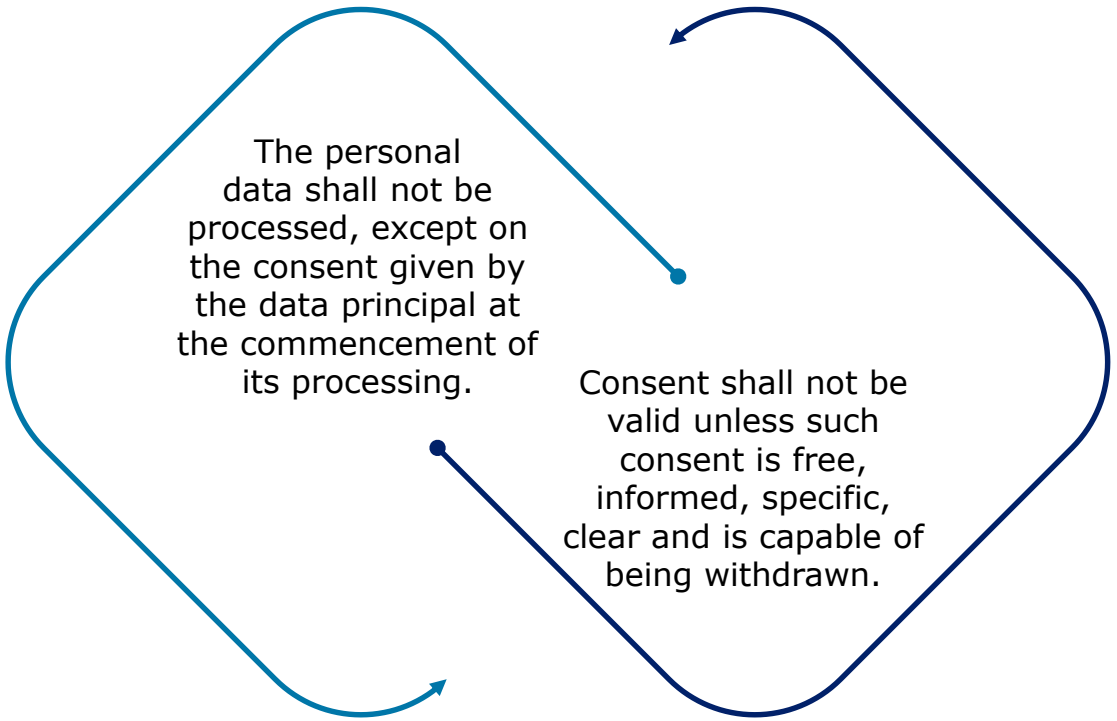
04 Clear and concise notice(in multiple languages where necessary) must be provided to the data principal at the time of collection of data.

05 Complete, accurate and updated data must be maintained by the data fiduciary

06 Time period for which data is retained must have a strong link with the purpose of processing.

Grounds for processing of personal data & sensitive personal data based on consent

Grounds for processing of personal data based on consent

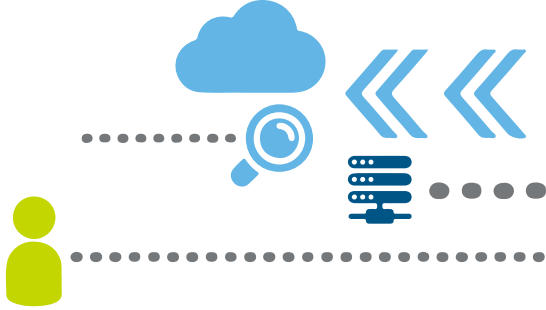


Grounds for processing of sensitive personal data based on consent

The consent of the data principal in respect of processing of any sensitive personal data shall be explicitly obtained -

1. after informing him the purpose of, or operation in, processing which is likely to cause significant harm to the data principal;
2. in clear terms without recourse to inference from conduct in a context; and
3. after giving him the choice of separately consenting to the purposes of, operations in, the use of different categories of, sensitive personal data relevant to processing.

Grounds for processing of personal data without consent



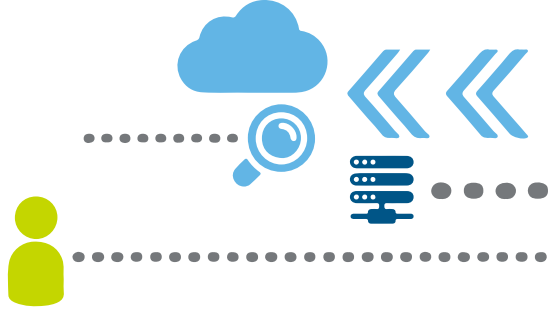
Grounds for processing of personal data without consent

Personal data maybe processed if such processing is necessary for :

1. Functions of the State
2. Compliance with law or any order of any court or tribunal
3. Respond to any medical emergency involving a threat to the life/ health of the data principal
4. Ensure safety of, or provide assistance or services to, any individual during any breakdown of public order
5. To provide medical treatment or health services to any individual
6. Purposes related to employment
7. Reasonable purposes

Without explicit consent, processing of sensitive personal data can not be practiced

Processing of personal data and sensitive personal data of children



Appropriate age verification and parental consent systems have to be incorporated by data fiduciaries before processing personal data and sensitive personal data related to children.

The manner for verification of the age of child shall be specified by regulations, taking into consideration -

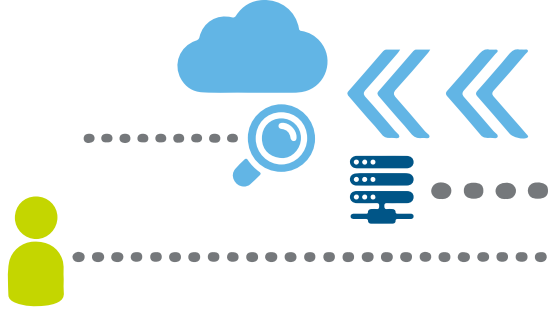
1. the volume of personal data processed
2. the proportion of such personal data likely to be that of child
3. possibility of harm to child arising out of processing of personal data
4. such other factors as may be prescribed

Data fiduciaries who operate commercial websites or online services directed at children or process large volumes of personal data of children

Guardian data fiduciaries

Guardian data fiduciaries will be prohibited from profiling, tracking or behavioral monitoring of or targeting advertising of children. Any other activity that may cause significant harm to the child is also barred.

Transparency and accountability measures



Privacy by Design Policy

Every data fiduciary shall prepare a privacy by design policy; Subject to the regulations made by the Authority, the data fiduciary may submit its privacy by design policy

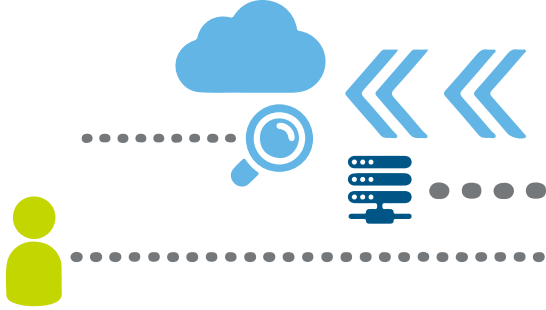
Transparency

The data fiduciary shall notify, from time to time, the important operations in the processing of personal data related to the data principal in such manner as may be specified by regulations.

Security Safeguards

Every data fiduciary and the data processor shall implement necessary security safeguards, having regard towards the nature, scope and purpose of processing personal data, the risks associated with such processing, and the likelihood and severity of the harm that may result from such processing to data principals.

Transparency and accountability measures



Personal Data Breach

In case of a personal data breach that is likely to cause harm to the data principal, the data fiduciary must notify the same to the Authority along with information with respect to the nature of the personal data that has been breached, number of data principals affected by the breach, consequences and measures taken to remedy the breach within the prescribed time frame.

Data Protection Impact Assessment

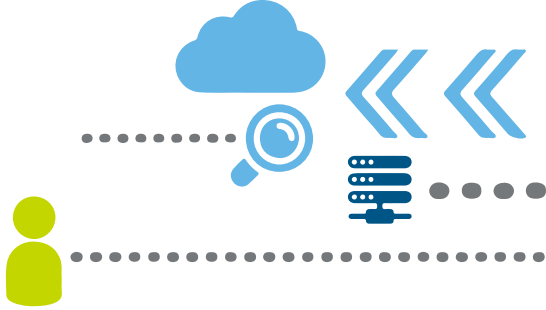
Where the significant data fiduciary intends to undertake processing involving new technologies, large scale profiling, use of sensitive personal data such as genetic data or biometric data, which carries a risk of significant harm to data principals, such processing shall not be commenced unless the data fiduciary has undertaken a data protection impact assessment in accordance with the provisions.

Record keeping and Data Audits

Accurate records of data lifecycle, periodic review of security safeguards and DPIA will have to be maintained by the data fiduciary.

The data fiduciary must have its policies and its processing activities audited annually by an independent auditor.

Transparency and accountability measures



Data Protection Officer and Grievance Redressal

- Every significant data fiduciary shall appoint a data protection officer possessing appropriate qualification and experience as per the regulation.
- The primary function of the DPO is to provide information and advice with respect to the data fiduciary's obligations under the Bill.
- The officer will assist the Authority to ensure compliance of the provisions by the data fiduciary.
- Every data fiduciary shall have in place the procedure and effective mechanisms to redress the grievances of data principals efficiently and in a speedy manner.

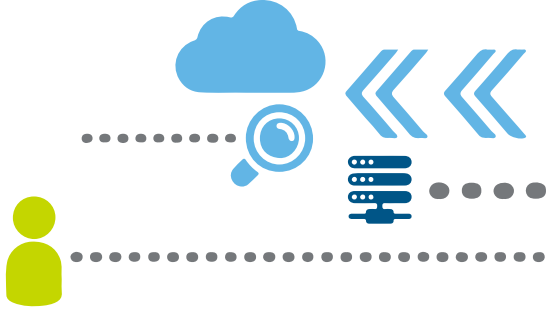
Processing by entities other than data fiduciary

Data fiduciaries must appoint a data processor to process personal data only through a valid contract. **Data Processors** must be prohibited from appointing sub processors without the consent of the data fiduciary and must treat personal data they are privy to as confidential.

Classification of data fiduciaries as significant data fiduciaries

- A notification of data fiduciary as a significant data fiduciary will be issued by the Authority based on the factors mentioned in the Bill.
- Any social media platform
  - i. with users above such threshold as may be notified by the Central Govt., in consultation with the Authority
  - ii. whose actions have, or are likely to have a significant impact on electoral democracy, security of the State, the sovereignty and integrity of India, shall be notified by the Central Government, in consultation with the Authority, as a significant data fiduciary.

Transfer of sensitive personal data

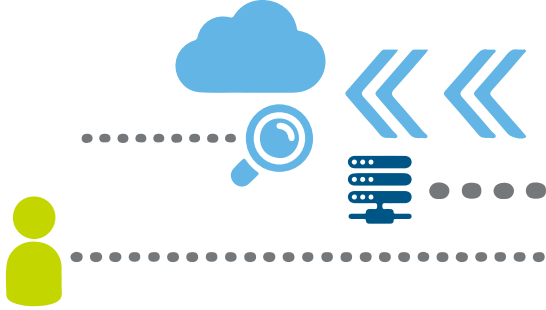


Sensitive personal data may only be transferred outside India for the purpose of processing, when **explicit consent is given by the data principal and consent from the DPIA** for such transfer, and where :

- The transfer is made pursuant to a contract or intra-group scheme approved by the Authority
- The Central Govt., after consultation with the Authority, has allowed the transfer to a country or, such entity or class of entity in a country or, an international organization
- The Authority has allowed transfer of any sensitive personal data or class of sensitive personal data necessary for any specific purpose

The Central government has the authority to categorize certain personal data as **critical personal data** and this data can only be processed in a server or a data Centre located in India.

Data protection impact assessment



DPIA has to be conducted in cases where the data fiduciary processes data involving new technologies, large scale profiling, sensitive personal data or processing that can risk significant harm being caused to the data principal.

Stages of DPIA

1. The Authority may, by regulations specified, such circumstances, or class of data fiduciary, or processing operation where such data protection impact assessment shall be mandatory, and also specify the instances where a data auditor shall be engaged by the data fiduciary to undertake a data protection impact assessment.
2. A DPIA must contain :
   i. A detailed description of the processing operation
   ii. Assessment of the potential harm that may be caused to the data principal
   iii. Measures to manage, mitigate or remove such harm to the data principal
3. Upon completion of DPIA, the data protection officer, shall review and submit the assessment with his findings to the Authority in such a manner as specified by regulations.

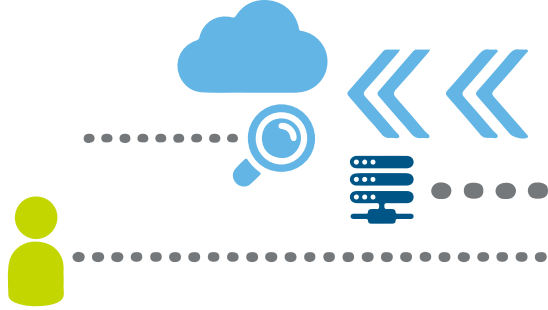
Cross border transfer of sensitive personal data

Cross Border Transfer

- The sensitive personal data may be transferred outside India, but such sensitive personal data shall continue to be stored in India.
- The critical personal data shall only be processed in India.
- The sensitive personal data may only be transferred outside India for the purpose of processing, when explicit consent is given by the data principal for such transfer, and where :
  1. The transfer is made pursuant to a contract or intra-group scheme approved by the Authority. Provided that such contract or intra-group scheme shall not be approved, unless it makes the provisions for—
     a) effective protection of the rights of the data principal under this Act, including in relation to further transfer to any other person; and
     b) liability of the data fiduciary for harm caused due to non-compliance of the provisions of such contract or intra-group scheme by such transfer;
  2. The Central Government, after consultation with the Authority, has allowed the transfer to a country or, such entity or class of entity in a country or, an international organization, on the basis of its findings that –
     a) such sensitive personal data shall be subject to an adequate level of protection, having regard to the applicable laws and international agreements;
     b) such transfer shall not prejudicially affect the enforcement of relevant laws by authorities with appropriate jurisdiction:

     Provided that any finding under this clause shall be reviewed periodically in such manner as may be prescribed;
  3. The Authority has allowed transfer of any sensitive personal data or class of sensitive personal data necessary for any specific purpose.
- Any critical personal data may be transferred outside India, only where such transfer is—
  1. to a person or entity engaged in the provision of health services or emergency services where such transfer is necessary for prompt action under section 12; or
  2. to a country or, any entity or class of entity in a country or, to an international organization, where the Central Government has deemed such transfer to be permissible and where such transfer in the opinion of the Central Government does not prejudicially affect the security and strategic interest of the State

Rights of data principles



Right to be forgotten

The right to be forgotten under the PDP Bill is essentially the right to prevent further disclosure of personal data, as it does not require the data fiduciary to erase the data but requires it to ensure erasure of data by data processors.

Right to Confirmation and Access

The data principal shall have the right to obtain from the data fiduciary—

a) confirmation whether the data fiduciary is processing personal data of the data principal;
b) the personal data of the data principal being processed by the data fiduciary,
c) a brief summary of processing activities

PDP Bill grants a wide range of rights to data principals that can be exercised :

Right to correction & erasure

The data principal shall where necessary, have the right to

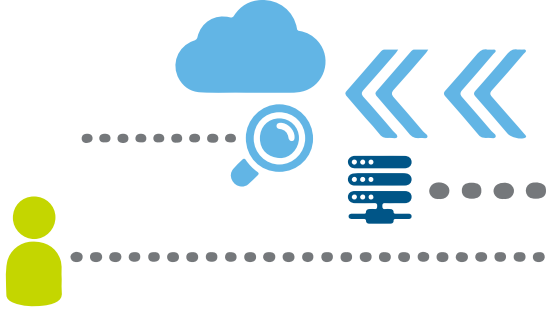
a) the correction of inaccurate or misleading personal data;
b) the completion of incomplete personal data;
c) the updating of personal data that is out-of-date; and
d) the erasure of personal data which is no longer necessary for the purpose for which it was processed.

Right to data portability

When processing is carried out through automated means, the data principal have the right to receive the following details regarding :

i. the personal data provided to the data fiduciary;
ii. the data which has been generated in the course of provision of services or use of goods by the data fiduciary; or
iii. the data which forms part of any profile on the data principal, or which the data fiduciary has otherwise obtained

Consent



Personal data may be processed on the basis of the consent of the data principal, and has to be given no later than at the commencement of the processing.

A valid consent would be -

- Free,
- Informed
- Specific, having regard to whether the data principal can determine the scope of consent in respect of the purposes of processing;
- Clear, having regard to whether it is indicated through an affirmative action that is meaningful in a given context; and
- Capable of being withdrawn, having regard to whether the ease of such withdrawal is comparable to the ease with which consent may be given.

Explicit consent- Sensitive personal data may be processed on the basis of explicit consent

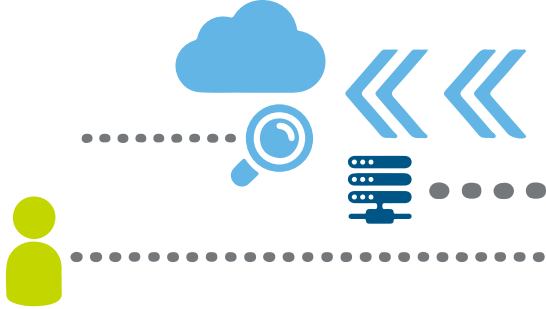
The data fiduciary shall bear the burden of proof to establish that consent has been given by the data principal for processing of personal data

If the data principal withdraws consent for the processing of any personal data necessary for the performance of a contract to which the data principal is a party, all legal consequences for the effects of such withdrawal shall be borne by the data principal

The data fiduciary shall not make the provision of any goods or services or the quality of those goods and services, performance of any contract, or the enjoyment of any legal right or claim, conditional on consent to processing of any personal data not necessary for that purpose.

The sensitive personal data may only be transferred outside India for the purpose of processing, when explicit consent is given by the data principal

Data breach notifications



Data Fiduciaries will have to:

Notify the Authority soon as possible and not later than the time period specified by the Authority of any personal data breach relating to any personal data processed by the data fiduciary where such breach is likely to cause harm to any data principal.

Include nature of personal data which is the subject matter of the breach, number of data principals affected by the breach, possible consequences of the breach and measures being taken by the data fiduciary to remedy the breach in the notification.

Take appropriate remedial action as soon as possible and to conspicuously post the details of the personal data breach on its website.

Upon receipt of notification, the Authority shall determine whether such breach should be reported by the data fiduciary to the data principal, taking into account the severity of the harm that may be caused to such data principal or whether some action is required on the part of the data principal to mitigate such harm.

Personal data breaches can result in high risks for the rights and freedoms of individuals. For Example: Identity theft, discrimination, fraud, damage to reputation, unauthorized reversal of pseudonymisation, loss of confidentiality of data protected by professional secrecy or any other significant societal or economic

Breach of Security leading to

+

The accidental or unlawful

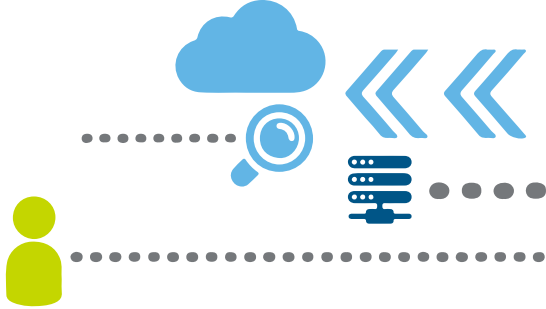
+

Destruction, loss, alteration, unauthorized disclosure of, or access to

+

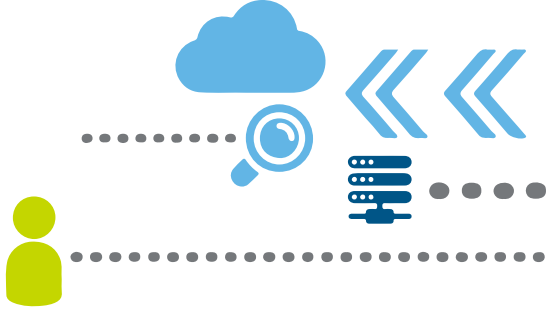
Personal data transmitted, stored or otherwise processed

Exemptions



01	02	03	04	05
Legal Proceedings	Personal or domestic purposes	Journalistic Purposes	Research, Archiving, Scientific or Statistical purposes	Processing by small entities
• Personal data is processed in the interests of prevention, detection, investigation and prosecution of any offence or any other contravention of any law for the time being in force; • Disclosure of personal data is for enforcing any legal right or, obtaining any legal advice from an advocate in any impending legal proceeding	• Personal data is processed by a natural person for any personal or domestic purpose, except where such processing involves disclosure to the public, or is undertaken in connection with any professional or commercial activity;	• This exemption will be applicable only in cases where the processing is in compliance with the code of ethics issued by the Press Council of India or any media self regulatory organization.	• This exemption is valid if the research, scientific or statistical activities are in compliance with the de-identification requirements and the said processed data is not used to make decisions in relation to data principals involved in the processing	• This exemption is applicable if personal data is processed by a company: • with a turnover not exceeding 20 lakh INR; • Which does not collecting personal data so as to disclose it to other individuals or entities; • Which does not process personal data of more than 100 data principals in one day in the last 12 months.

Penalties and remedies



Penalties

- Fine up to INR 5 Crore or 2% of worldwide turnover of the preceding financial year (whichever is higher)
- Fine up to INR 15 crore or 4% of worldwide turnover (whichever is higher)
- Where, any data fiduciary, without any reasonable explanation, fails to comply with any request made by a data principal, such data fiduciary shall be liable to a penalty of five thousand rupees for each day during which such default continues, subject to a maximum of ten lakh rupees in case of significant data fiduciaries and five lakh rupees in other cases.

Remedies

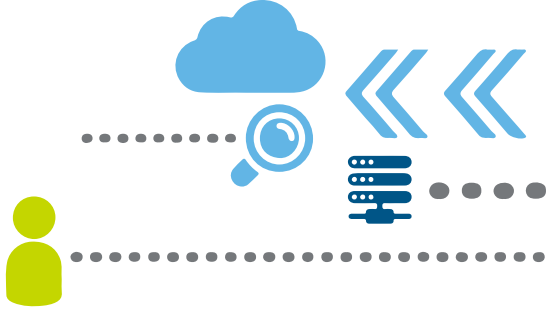
- A data principal can seek to redress its grievance by approaching the Data Protection Officer and the grievance should be addressed within 30 days from the date of complaint.
- The data principal if dissatisfied with the ruling of the officer can also approach the Appellate Tribunal.
- The data principal can also approach the Supreme Court if it is dissatisfied with the order of the Appellate Tribunal
- The data principal cannot approach a civil court for remedy and no injunction can be granted by the officer, Supreme Court or the Tribunal.

Compensation

A data principal who has suffered harm has the right to seek compensation from the data fiduciary or the data processor and the amount of compensation depends on:

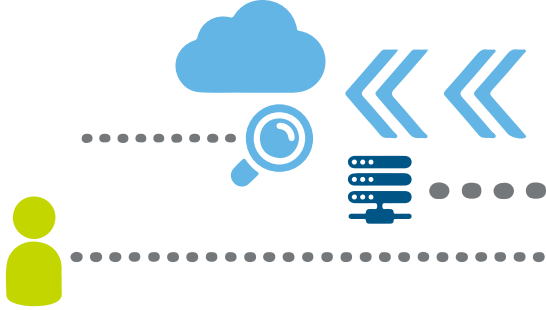
a) nature, duration and extent of violation;
b) nature and extent of harm suffered by the data principal;
c) intentional or negligent character of the violation;
d) transparency and accountability measures implemented by the data fiduciary or the data processor, as the case may be, including adherence to any relevant code of practice relating to security safeguard;
e) action taken by the data fiduciary or the data processor, as the case may be, to mitigate the damage suffered by the data principal;
f) previous history of any, or such, violation by the data fiduciary or the data processor, as the case may be;
g) whether the arrangement between the data fiduciary and data processor contains adequate transparency and accountability measures to safeguard the personal data being processed by the data processor on behalf of the data fiduciary

Offences



Offences	Quantum of punishment
Re-identification & Processing of de-identified personal data	
Any person who, knowingly or intentionally— a) re-identifies personal data which has been de-identified by a data fiduciary or a data processor, as the case may be; or b) re-identifies and processes such personal data as mentioned in clause (a) , without the consent of such data fiduciary or data processor.	Such person shall be punishable with imprisonment for a term not exceeding three (3) years or with a fine which may extend to two (2) lakh rupees or both.
Cognizable and non-bailable offences	
1. Notwithstanding points contained in the Code of Criminal Procedure, 1973, an offence punishable under this Act shall be cognizable and non- bailable. 2. No court shall take cognizance of any offence under this Act, save on a complaint made by the Authority.	
Offences by Companies	
Where an offence under this Act has been committed by a company, every person who, at the time the offence was committed was in charge of, and was responsible to, the company for the conduct of the business of the company, as well as the company, shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.	Depends on the nature of offence (refer above)
Offences by Central of State Government Departments	
Where it has been proved that an offence under this Act has been committed by any department or authority or body of the State, by whatever name called, the head of such department or authority or body shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.	Depends on the nature of offence (refer above)

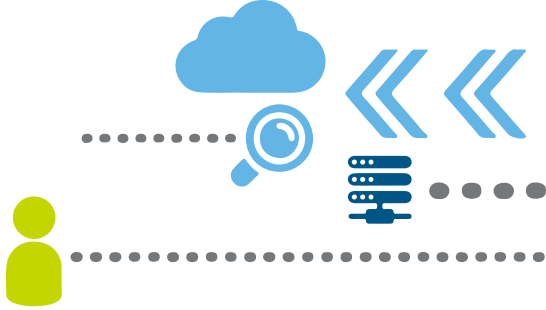
Data Protection Authority of India



Powers and Functions of Authority

- The Authority would be set up by the Central Government
- The appointments and associated terms and conditions for the authority will be taken care by the Central Government
- The Authority shall, by regulations, specify codes of practice to promote good practices of data protection and facilitate compliance with the obligations under this Act.
- Without prejudice to the generality of the foregoing and other functions under this Act, the functions of the Authority shall include
  a) monitoring and enforcing;
  b) taking prompt and appropriate action in response to personal data breach in accordance with the provisions of this Act;
  c) maintaining a database on its website containing names of significant data fiduciaries along with a rating in the form of a data rust score indicating compliance with the obligations of this Act by such fiduciaries;
  d) examination of any data audit reports and taking any action pursuant thereto;
  e) issuance of a certificate of registration to data auditors and renewal, withdrawal, suspension or cancellation thereof and maintaining a database of registered data auditors and specifying the qualifications, code of conduct, practical training and functions to be performed by such data auditors;
  f) classification of data fiduciaries;
  g) monitoring cross-border transfer of personal data;
  h) specifying codes of practice;
  i) promoting awareness and understanding of the risks, rules, safeguards and rights in respect of protection of personal data amongst data fiduciaries and data principals;
  j) monitoring technological developments and commercial practices that may affect protection of personal data;
  k) promoting measures and undertaking research for innovation in the field of protection of personal data;
  l) advising Central Government, State Government and any other authority on measures required to be taken to promote protection of personal data and ensuring consistency of application and enforcement of this Act;
  m) specifying fees and other charges for carrying out the purposes of this Act;
  n) receiving and inquiring complaints under this Act; and
  o) performing such other functions as may be prescribed.

Appellate tribunal



Powers & Functions of the Tribunal

- The Central Government will establish the Tribunal
- The Central Government will be responsible for the appointments and setting up of benches in relation to the Tribunal
- Orders passed by the Tribunal will executable as a decree
- Civil Courts will have no jurisdiction
- Appeal from the orders of the Tribunal will be taken up by the Supreme Court

a) Summoning and enforcing the attendance of any person and examining that person on oath;
b) Requiring the discovery and production of documents;
c) Receiving evidence on affidavits;
d) Requisitioning any public record or document or a copy of such record or document, from any office;
e) Issuing commissions for the examination of witnesses or documents;
f) Reviewing its decisions;
g) Dismissing an application for default or deciding it, ex parte;
h) Setting aside any order of dismissal of any application for default or any order passed by it, ex parte (without the presence of parties);
i) Proceedings of Tribunal will be deemed as judicial proceedings under the Indian legal framework.

Deloitte.