jsa
advocates & solicitors

Knowledge Management

Digital Personal Data Protection Act Compendium 2024

Contents

Applicability of the Digital Personal Data Protection Act, 2023 and the roles thereunder

Material Scope

The subject matter that the Digital Personal Data Protection Act, 2023 ("**DPDPA**") regulates is the material scope. The DPDPA applies to the processing of digital personal data.

1. Personal data, as defined under the DPDPA, means any data about an individual who is: '*Identifiable by such data*' where the personal data, by itself can directly identify an individual. For example, if the data includes a person's name, or an email address that can directly reveal their identity; or '*identifiable in relation to such data*' where the data relates to an individual but may not directly identify them without additional information. For example, IP address when combined with other data, leading to the identification of an individual.
2. The DPDPA only applies to 'digital' personal data i.e., means personal data that is collected in a digital form or collected in physical form and digitised subsequently.

The DPDPA does not further categorize 'sensitive' personal data separately.

Territorial Scope

The DPDPA applies to the processing of personal data '*within the territory of India'* and '*outside the territory of India'* subject to fulfilment of certain conditions.

When is processing of personal data in India covered?

DPDPA applies to the processing of digital personal data happening within the territory of India.

- If an entity carries out the processing activity in India, then DPDPA will apply to processing of personal data by that entity, irrespective of the residency of that entity or of the data principal.
- If the processing occurs within the territory of India, it is immaterial if it is connection with offering goods or services to the data principals.

When is processing of personal data outside India covered?

When the processing is '*in connection with any activity related to offering of any goods or services offered to data principals in India'*, the DPDPA is applicable.

Where the processing happens outside India but data principals in India are targeted '*in connection with any activity related to offering of goods or services'* which could be advertising, marketing/promotional activities, sales, availability in, handling inquiries etc, the DPDPA applies to such processing.

The General Data Protection Regulation ("**GDPR**") has a similar provision where the GDPR applies to an entity not established in the European Union ("**EU**") where the processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the EU.

When is the DPDPA not applicable?

Non-applicability of the DPDPA.

(a) If the personal data is processed for any personal or domestic purpose.

Where the processing of personal data has no connection to a professional or commercial activity.

(b) If the personal data that is made or caused to be made publicly available by:

the data principal to whom such personal data relates;

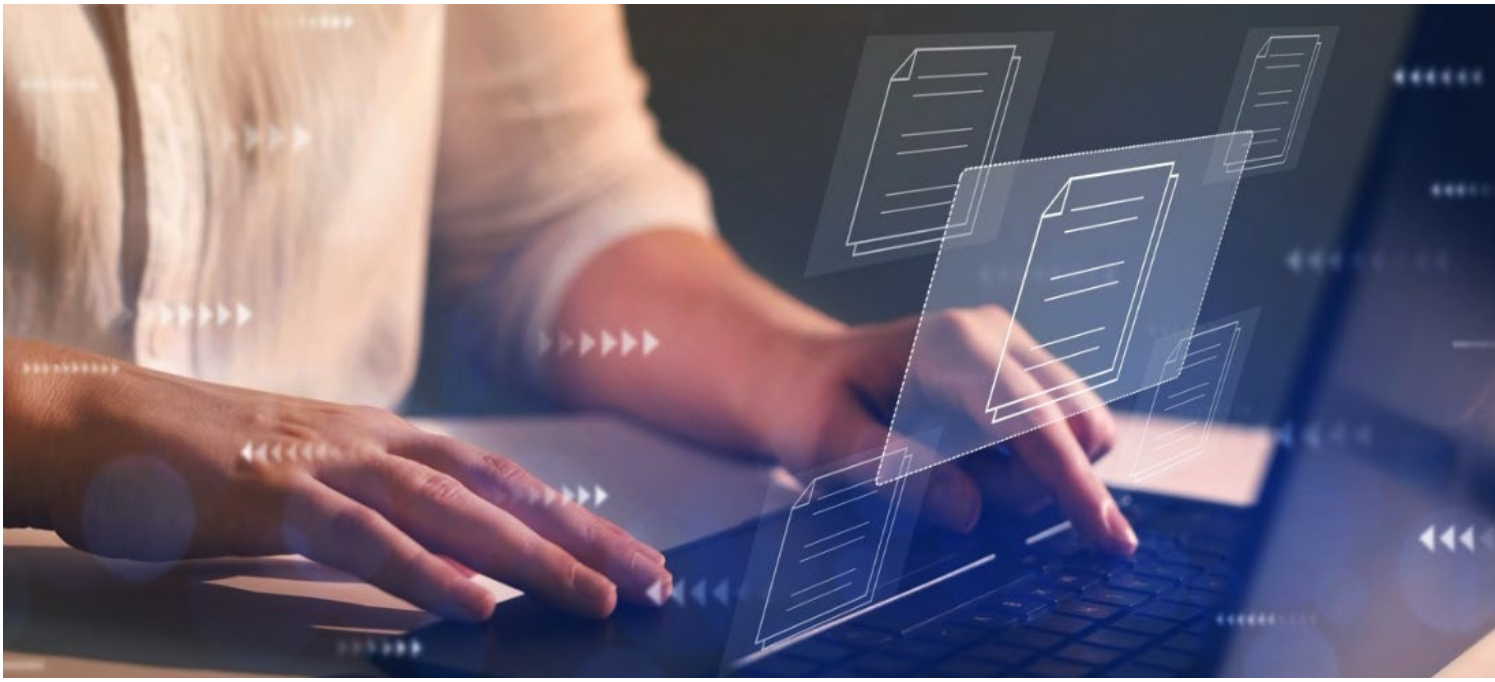
Where the data principal themselves have made the personal data public or directed to make the personal data available to the general public.

OR

any other person who is under a legal obligation to make such personal data publicly available.

Where a person is legally required to make the personal data public.

- Similar to the DPDPA, the California Consumer Privacy Act ("**CCPA**") also excludes *'publicly available information*' from the definition of personal information. '*Publicly available information*' is defined as data from government records, information publicly shared by the consumer or media, or information shared by the consumer unless restricted to a specific audience but excluding biometric information. Under the GDPR, the general prohibition on processing special categories of data does not apply to personal data manifestly made public by the data subject.
- Although processing of personal data available publicly is exempted under the DPDPA, the processing of such personal data will have to be in compliance with other applicable laws, for example, the Information Technology Act, 2000 or Intellectual Property laws.



What are the different roles a person processing personal data could play under the DPDPA?

Data Fiduciary

- Any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.
- **A Person:** This term has been defined under the DPDPA and includes individuals, companies, a HUF, government agencies, or any other legal entities.
- **Who 'alone' or 'in conjunction with' other Persons:** A person that independently makes decisions about the processing of personal data or multiple persons collaborating or jointly making decisions about the processing of personal data.
- **Determines the Purpose And Means of Processing:** Makes decisions on what personal data is being processed, for what purpose, how and where the personal data is stored and protected, etc

Data Principal

- **The individual to whom the personal data relates:** This refers to the natural person whose personal data is being processed.
- **If the data principal is a child, includes the parents or lawful guardian of that child:** A child in this context is someone below 18 years of age. A child's parents or lawful guardians are to make decisions regarding the child's personal data on their behalf.
- **If it is a person with a disability, includes their lawful guardian acting on their behalf:** refers to individuals with 'disability' as defined under applicable laws. For persons with disabilities, their lawful guardian is responsible for making decisions regarding the individual's personal data on their behalf

Data Processor

- means any person who processes personal data on behalf of a data fiduciary.
- **'On behalf of a data fiduciary'** means that the processing activities are carried out not for the processor's own purposes but on behalf of and for the purposes set by the data fiduciary.

Unlike the GDPR, there is no separate concept of a "joint controller/joint fiduciary" under the DPDPA. Each data fiduciary is responsible for compliance with their obligations under the DPDPA.

Comparison with select data protection laws around the world

Concept	DPDPA	GDPR	CCPA	Personal Data Protection Act ("PDPA"), Singapore
Intra-Territorial Applicability	The DPDPA is applicable to processing of digital personal data in the territory of India.	The GDPR applies to controllers or processors established in the EU, irrespective of whether the data processing takes place in the EU or not.	A for-profit business that carries out business in California and meets one of the following thresholds is subject to CCPA: has annual revenue of over USD25 million, or collects personal information of over 100,000 California residents, or generates at least half of its revenue from selling personal information of California residents.	The PDPA applies to all organisations which are not a public agency that undertakes processing of personal data in Singapore whether or not the organisation has been registered under the laws of Singapore.
Extra-territorial Applicability	The DPDPA applies to processing that happens outside India if it is in connection with offering goods or services to individuals in India.	The controllers and processors outside the EU fall within the ambit of GDPR if they are offering goods or services to individuals who are in the EU or if they monitor the behaviour of residents in the EU.	The CCPA is applicable to businesses outside California if they do business in California (that includes offering goods or services) and satisfies one of the thresholds.	The PDPA is applicable to organisations that collects, uses and discloses personal data in Singapore whether or not formed or recognised under the laws of Singapore.
Publicly available personal data	The DPDPA is not applicable to personal data made public by the data principal or by any person under a legal obligation to make such data public.	The GDPR is applicable to personal data made publicly available by the data subjects.	The CCPA has a restricted definition of publicly available information. It means information available from government records, information that has been lawfully made public by the consumer or widely distributed media, or information made available by the consumer unless they have restricted it to a specific audience.	The PDPA provides certain exceptions for publicly available personal data such as collection, use, or disclosure of such personal data can be done without the consent of the individual.
Stakeholders	Data Fiduciary, Data Processor, Data Principal.	Data Controller, Data Processor, Data Subjects.	Business, Service Provider, Consumer.	Organisation, Data Intermediary, Individual.
Nature of personal data protected	The DPDPA protects only digital personal data.	The GDPR protects personal data in both digital and physical formats	The CCPA applies to processing of personal data in both digital and physical formats.	The PDPA regulates personal data collected both in digital and non-digital formats

Legal basis of processing and privacy notice

Legal basis for processing

The processing of personal data should be for lawful purposes. A lawful purpose is a purpose that is not expressely fobidden by law.

The lawful processing should be upon the consent of the data principal

'*Consent*' must be free, specific, informed, unconditional and unamiguous with a clear affirmative action.

OR

Personal data can be processed without the data principal's consent if it is for any of the 'legitimate uses' mentioned in Section 7 of the DPDPA.

- Consent can be obtained through an interoperable platform called a 'consent manager', more details of which will be provided in the Rules
- It is pertinent to identify the right legal basis for processing since the notice requirements and the data principals' rights will differ based on the legal basis.
- DPDPA does not categorise sensitive personal data separately. Therefore, there are no specific grounds for processing of sensitive personal data, unlike the GDPR.

What are the '*Legitimate Uses*'?

The DPDPA lists 9 (nine) legitimate uses, where personal data can be processed without the consent of the data principal.

Voluntary Basis:

Where the data principal has voluntarily provided the personal data for a specified purpose	The data principal should have provided the personal data for a particular purpose, of their own accord.
in respect of which she has not indicated that she does not consent to the use of her personal data	The data principal has not indicated to restrict the processing of their personal data.

What will be considered as 'voluntary' provision of personal data is ambiguous.

Processing by the State or its instrumentalities:

The processing of personal data by the Government or its departments for provinding benefits, subsidies, certificates, licenses, etc to data principals only if one of the two conditions is satisfied.

Rules will be made for this section giving more details on the use by the Government

- (a) Where the data principal has already given consent for their personal data to be processed by the Government for providing such services.
- (b) If the digital personal data is already present in the Government's databases.

Any processing by the Government or its departments must also comply with policies issued by the Central Government or any law in force that regulates governance of personal data.

Processing for State Functions:

The processing of personal data is necessary for the Government or its departments to perform its functions as mandated under law

or if the processing of personal data is necessary in the interest of sovereignty and integrity of India or security of India.

Processing for Fulfilling Legal Obligations:

The processing of personal data, without consent, is allowed if it is required to comply with an obligation that is required by law in India

This processing and disclosure of information must comply with the specific provisions and regulations set out in any relevant laws that are currently in force.

Processing for Compliance with Court Orders:

Processing of Personal Data is allowed for compliance with any decree, judgement or order passed by an Indian Court.

Or for compliance with any judicial order passed by courts outside India if they relate to any contractual or civil claims.

Processing during Medical Emergencies:

Personal data may be processed, without consent, for responding to a medical emergency that is a threat or immediate threat to the health of a data principal or any other individual.

Processing during Epidemic or Outbreak of Disease

Personal data may be processed, without consent, for taking actions or steps to provide medical treatment or health services to any individual during an epidemic, disease outbreak or other threat to public health.

Processing during Disaster or Breakdown of Public Order

Processing can be done, without consent, for taking measures to ensure safety of, or provide assistance or services to any individual during any 'disaster' or breakdown of public order

'Disaster' is defined under the Disaster Management Act of 2005 as *"a catastrophe, mishap, calamity or grave occurrence in any area, arising from natural or man-made causes, or by accident or negligence which results in substantial loss of life or human suffering or damage to, and destruction of, property, or damage to, or degradation of, environment, and is of such a nature or magnitude as to be beyond the coping capacity of the community of the affected area".*

Processing for the Purpose of Employment

Processing can be done, without consent, for the purposes of employment, which may include activities like hiring, undertaking background checks, managing the employee, termination, or those related to safeguarding employer from loss or liability.

Processing can be done, without the employee's consent, to take action to prevent theft of employer's proprietary information, or trade secrets and to maintain confidentiality of data

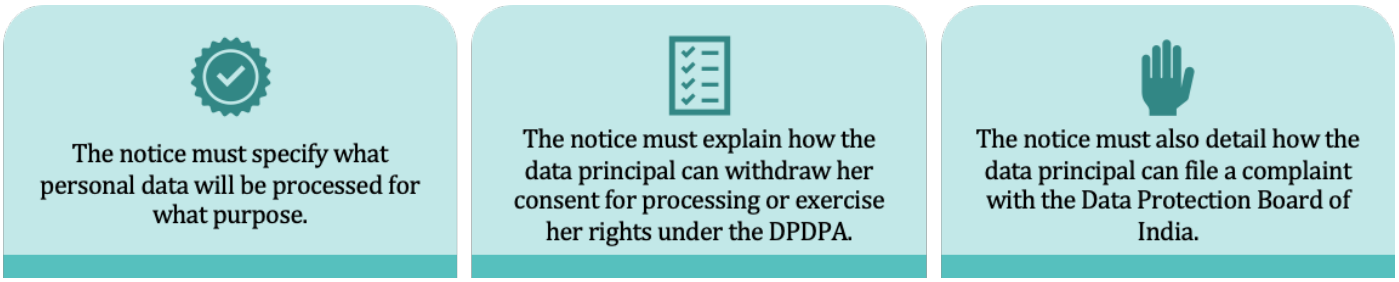
Processing can be done, without employee's consent for provision of any service or benfit sought by the employee.

- There is lack of clarity on whether the term '*for employment purposes*' can be extended to contractors, retainers or professionals.
- In a similar context, the PDPA of Singapore specifically allows processing of personal data (without obtaining consent) to evaluate the individual or to manage or terminate the employment relationship.

Notice under the DPDPA:

a) A notice should be provided to the data principal while requesting their consent or to identify the purpose if the personal data is volunteered.

b) *What should be the contents of a notice?*



c) The notice must be provided earlier than or along with the request for consent.

d) Where a data principal has given her consent for the processing of her personal data before the date of commencement of the DPDPA, a notice should be provided to the data principal as soon as it is reasonably practicable. The data fiduciary may continue to process the personal data until the data principal withdraws their consent.

e) The data fiduciary will give the data principal the option to access the contents of the notice in English or in any language specified in the Eighth Schedule to the Constitution of India.

f) The Rules will prescribe the manner in which the notice should be given to the data principal.

It is not clear if the notice has to be provided in all the languages that are listed on the Eighth Schedule in the Constitution of India, as it may be *an operational overhead. Currently, there are* 22 (twenty-two) languages in this Schedule vis.: Assamese, Bengali, Bodo, Dogri, Gujarati, Hindi, Kannada, Kashmiri, Konkani, Malayalam, Manipuri, Marathi, Maithili, Nepali, Oriya, Punjabi, Sanskrit, Santhali, Sindhi, Tamil Telugu, and Urdu.

Comparison with select data protection laws around the world:

Concept	DPDPA	The GDPR	The California Consumer Privacy Act	PDPA, Singapore
Legal basis for processing personal data	Consent or legitimate uses	Consent, necessary for fulfilment of contractual obligations, for compliance with legal obligations, for protecting the vital interests of the data subject, necessary for performance of task carried out in public interest or legitimate interests.	There is a general presumption that a business can process personal data without relying on a legal basis. However, businesses are required to provide an option to the consumers to opt-out from selling or sharing of their personal information.	Consent, or without consent for circumstances mentioned in the PDPA. It is an exhaustive list, some of the instances are where it is necessary to protect vital interests of the individual, necessary in national interest, processing for artistic, literary, archival, research or historical purposes, for the legitimate interest of the organisation, necessary for investigation or proceedings, for employment purposes, for the purposes of business asset transaction, for business improvement purposes, etc.
Legal basis for processing of sensitive personal data	DPDPA does not define sensitive personal data. Hence there are no specific legal bases for processing it.	GDPR prohibits the processing of special categories of personal data unless the consent of the data subject is obtained or one of the conditions mentioned	Sensitive personal information can be processed without consumer's consent, but businesses must offer consumers the option to limit its use	The PDPA does not mention specific legal basis for processing of sensitive personal data.

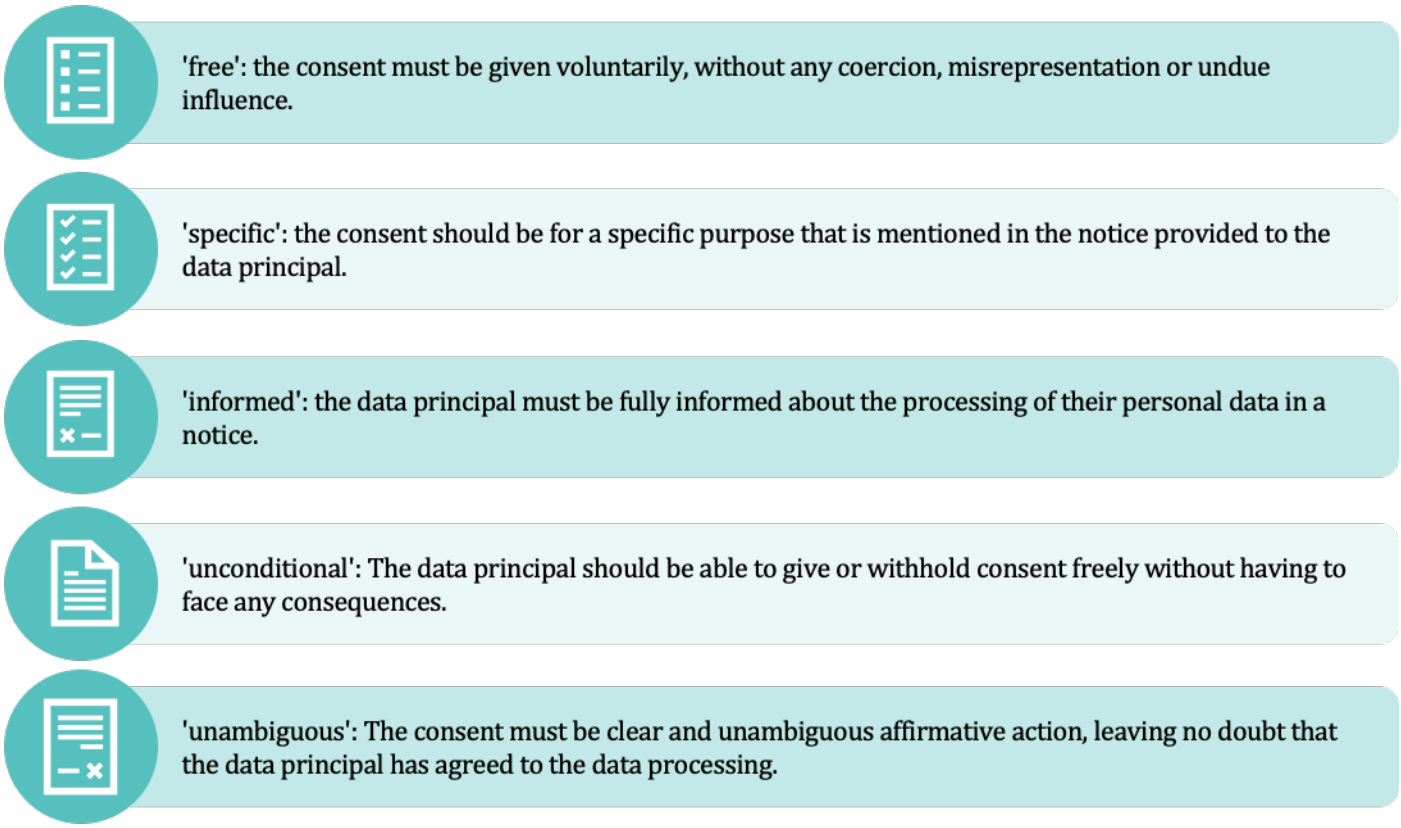
Concept	DPDPA	The GDPR	The California Consumer Privacy Act	PDPA, Singapore
		under Article 9 of GDPR is fulfilled.	or prevent sharing and selling.	
Notice	A notice will have to be provided to the data principal when requesting consent, or to notify the specific purpose when the data principal volunteers their data. Notice will also have to be given for personal data obtained before the commencement of the DPDPA.	When personal data is collected directly or indirectly from the data subject, notice must be provided regardless of the legal basis for processing. However, notice is not required in certain circumstances, such as when an individual already has the information, if providing notice would involve disproportionate effort, if the law permits obtaining or disclosing the personal data, or if confidentiality is mandated due to professional secrecy law.	A business must provide notice at or before the collection of a consumer's personal information. If the business does not collect personal information directly from the consumer and does not sell or share it, no notice is required.	Notice must be provided when obtaining an individual's consent, except when consent is 'deemed' or other legal bases are relied upon.

Consent and Consent Managers

What is "consent" and what are the key elements of a valid consent?

Consent is considered as the primary ground that allows processing of personal data. A valid consent must fulfil the following requirements:

Consent must be:



The consent should signify that the data principal agrees to the processing of their personal data for the purpose mentioned in the notice given by the data fiduciary to the data principal. Consent should also be obtained only for personal data that is necessary for the specified purpose.

- The consent must indicate a clear affirmative action which means actively ticking a box or signing a document. Therefore, passive actions like pre-checked boxes or call-to-actions may not count as a valid consent.
- The CCPA mentions that acceptance of general or broad terms of use, hovering over, muting, pausing or closing a tab, or consent that have been obtained through dark patterns cannot be considered as a valid consent. Similarly, the GDPR also mentions that pre-ticked boxes or inactivity will not be considered as consent.
- Since the DPDPA mentions that consent should be given for specific purposes, granular options may be given to consent separately to separate purposes.

When is a consent invalid?

To the extent that a consent infringes the DPDPA, its rules or any other law in India, it shall be invalid to that extent.

How should a request for a consent be made?

The request for consent

- should be made in a clear and plain language.
- shall be made accessible either in English or any language mentioned in the Eighth schedule of the constitution of India.
- should provide the contact details of a data protection officer, or any other person who will respond to any requests or queries from the data principal to exercise their rights provided under the DPDPA.

1. **Right to withdraw consent**: Where the data fiduciary relies on consent to process the personal data, data principal will have the right to withdraw her consent at any time.

- Such withdrawal of consent must be as easy as the process of giving consent. There should not be any unnecessary hurdles or complications that make it difficult for the data principal to withdraw their consent.
- The consequences of the withdrawal will have to be borne by the data principal.
- The withdrawal of consent will not affect the legality of the processing that happened before the withdrawal.
- The data fiduciary will ensure within a reasonable time, that it stops the processing of personal data for which the data principal has withdrawn their consent and ensure that its data processors also stop processing the personal data unless the processing relies on legitimate uses or the processing is required under any law in India.

2. **Record keeping**: If a question arises on the legality of the consent provided by the data principal, the data fiduciary must be able to demonstrate that a notice was given by the data fiduciary to the data principal and consent was given by the data principal in accordance with the DPDPA.
3. The data principal may give, manage, review or withdraw her consent to the data fiduciary through a 'Consent Manager'.

   Who is a 'Consent Manager'?

   A consent manager has been defined as a person registered with the Data Protection Board of India ("**Board**"), who acts as a single point of contact to enable data principals to '*give, manage, review and withdraw*' the data principal's consent through '*an accessible, transparent and interoperable platform*'.

1. The consent manager will have to be accountable to the data principal.
   - The rules will provide the manner in which the consent managaer will be accountable to the data principal.
2. The consent manager will act on behalf of the data principal.
   - The rules will provide the manner in which the consent manager will act and the obligations of the consent manager.
3. The consent manager should be registered with the Board and comply with any technical, operational, financial and other conditions as prescribed by the Board.
   - The rules will provide the manner of registration and the conditions for such registration of the consent manager with the Board.
4. The consent manager should also provide the data principal with readily available means of grievance redressal against any acts or omission of the consent manager regarding: (a) performance of its obligations or (b) exercise of the data principal's rights under the DPDPA.
5. The consent manager should respond to the grievances of the data principals within the prescribed time limit.

- Similar to the DPDPA, the Account Aggregator ("**AA**") Framework by the RBI allows AAs to act as intermediaries that obtain, submit and manage the consent of users to obtain their financial data from banks and share it with lending institutions. Similarly, the National Digital Health Mission's health data management policy also has the concept of consent managers to manage consent for health data.
- It is unclear whether consent managers will also collect personal data alongside obtaining consent.
- It is also pertinent to know if the Electronic Consent Framework (released by the Ministry of Electronics and Information Technology ("**MeitY**") in 2017) will be made applicable to consent managers since the document outlines technology specifications to manage user consent provided electronically to share data across different entities.

Comparison with select data protection laws around the world

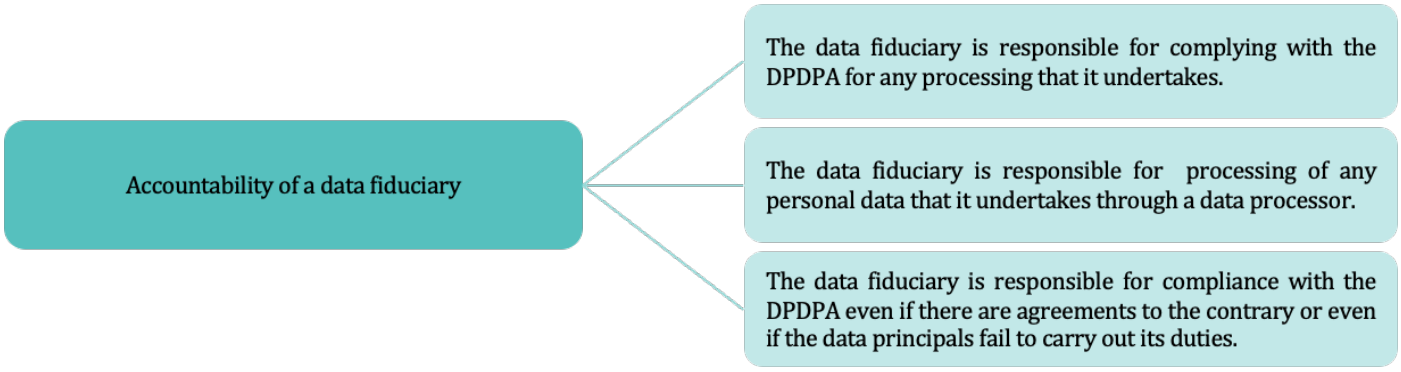
Concept	DPDPA	GDPR	CCPA	PDPA
Consent and its key elements	The consent given by the data principal will be free, specific, informed, unconditional and unambiguous with a clear affirmative action, and will signify an agreement to the processing of personal data for the specified purpose and will be limited to such personal data as is necessary for such specified purpose.	Under GDPR, consent should be freely given, specific, informed, unambiguous and will be an affirmative action.	Consent must be freely given, specific, informed and unambiguous. Consent will be a clear affirmative action provided for processing personal information for a narrowly defined purpose.	While requesting for consent, the individual should be provided with information such as the purpose for the processing and any secondary purpose of processing, and the consent should be obtained only for a specific purpose.
Aspects of Consent	• Every request for consent will be in a clear and plain language providing the option to access the notice in English or in any language in the Eighth Schedule. It will provide details of the Data Protection Officer or authorised person. • Consent can be withdrawn, but the consequences will have to be borne by the data principal. • If the consent is withdrawn, the same will not affect the legality of processing before its withdrawal. • Post withdrawal of the consent, the data fiduciary will stop processing of personal data and ensure the data processors also stop the processing. • The data fiduciary must be able to evidence that a notice was given by the data fiduciary to the data principal and consent was given by the data principal in accordance with the DPDPA.	• The controller will keep records to demonstrate that consent has been obtained. • Request for consent will be in an intelligible and easily accessible form, using clear and plain language. • The data subject should be able to withdraw the consent at any time. • The performance of a contract should not be condition on consenting to the processing of personal data that is not necessary for the performance of the contract.	Consent can be revoked: • when such consent was provided for receiving financial benefit, • when consent was initially provided to allow the business to ignore the opt-out preference signal with respect sale or sharing of the personal information or the use of the consumer's sensitive personal information.	• The individual can withdraw consent at any time. • Consent will not be obtained as a condition to provide a product or service if the same is beyond what is reasonable to provide the product or service.
Consent Manager	The concept of consent manager is introduced in DPDPA. They are a person registered with the Board, who	GDPR does not make a reference to consent managers, however it does allow individuals	Although there is no concept of consent manager in the CCPA,	PDPA mentions that the consent may be given by any person validly

Concept	DPDPA	GDPR	CCPA	PDPA
	acts as a single point of contact to enable a data principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform.	who have the authority to act on behalf of data subjects when they are incapable of providing consent to manage consent on their behalf.	consent can be given by the consumer, their legal guardian or a person who has power of attorney, or person acting as a conservator for the consumer. However, a consumer may authorize another person to opt out of the sale or sharing of the consumer's personal information and to limit the use of the consumer's sensitive personal information on the consumer's behalf.	acting on that individual's behalf.

General obligations of data fiduciaries and significant data fiduciaries

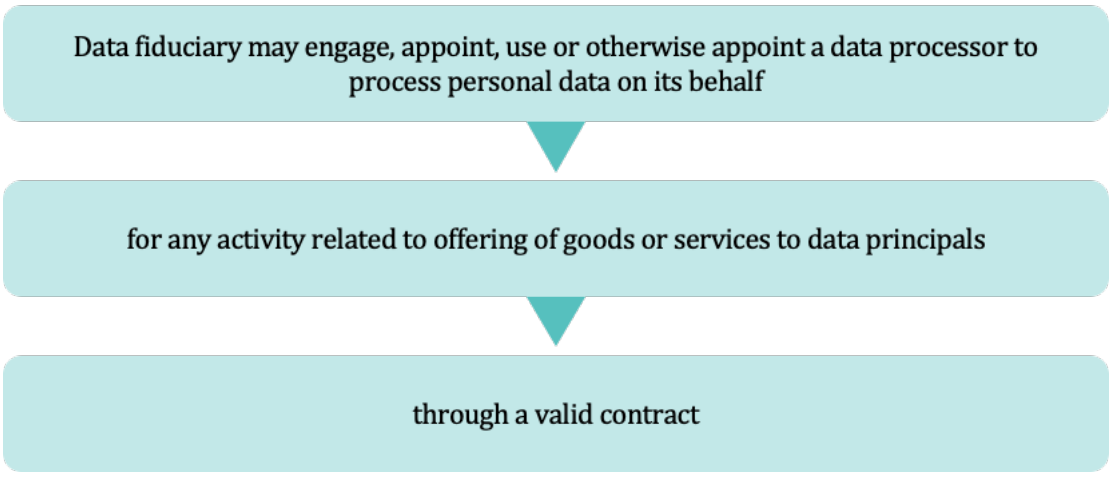
What are the obligations of a data fiduciary?

Accountability:



- Data processors are defined under the DPDPA to mean any person who processes personal data on behalf of a data fiduciary.
- It is pertinent to note that unlike the GDPR the data processors do not have any direct obligations under the DPDPA. The data fiduciary is responsible for the compliance of the data processors. Therefore it is important to undertake due diligence on data processors before their appointment.
- The DPDPA does not mandate maintaining a Record of Processing Activities ("**ROPA**"). However maintaining a ROPA will help in identifying gaps in compliance with the DPDPA, and it will also help in responding to data principals' access rights.
- The GDPR mentions that a controller can demonstrate compliance with the GDPR by implementing internal data protection policies, by adhering to code of conduct or certification mechanism. However, the DPDPA does not explicitly mention any measures by which data fiduciary can demonstrate compliance with its obligations.

Engagement of data processors:



Ensuring completeness, accuracy and consistency of personal data:

The data fiduciary should ensure the completeness, accuracy and consistency of personal data when it is likely to be

(a) used to make a decision that affects the data principal;

OR

(b) disclosed to another data fiduciary.

Implementing technical and organizational measures:

A data fiduciary should implement appropriate technical and organisational measures

to ensure effective compliance with the DPDPA and the rules.

- The GDPR mentions implementing privacy by design and default and other measures like pseudonymising personal data or encryption of personal data as an example of implementing measures to meet the principles of data protection. However, the DPDPA does not elaborate upon the technical and organisational measures for compliance with the DPDPA.
- The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**SPDI Rules**") state that body corporates which have implemented the international standard IS/ISO/IEC 27001 or followed data protection best practice codes provided by an association are deemed to have complied with reasonable security practices and procedures. However, the DPDPA does not provide any such standards for demonstrating compliance.

Protection of personal data:

The data fiduciary should protect personal data in its possession or under its control by implementing measures.

The measures may include directing the data processors to take reasonable security safeguards to prevent personal data breach.

Intimation of personal data breach:

In the event of a personal data breach, the data fiduciary should

(a) notify the Data Protection Board

(The Rules will prescribe the form and manner to notify the board).

(b) notify the affected data principals.

Contact details of the Data Protection Officer ("DPO") or authorized person of the data fiduciary:

The data fiduciary should publish:

- (a) The contact details of the DPO if applicable

  (The rules will mention the manner of publishing the business contact information of a DPO.)
- (b) If appointment of a DPO is not applicable, then the details of the personnel who can answer the questions raised by the data principal on behalf of the data fiduciary.

Effective grievance redressal mechanism:

Data fiduciaries should establish an effective mechanism to redress the grievances of data principals.

Retention of personal data:

A data fiduciary should delete the personal data upon the earlier of

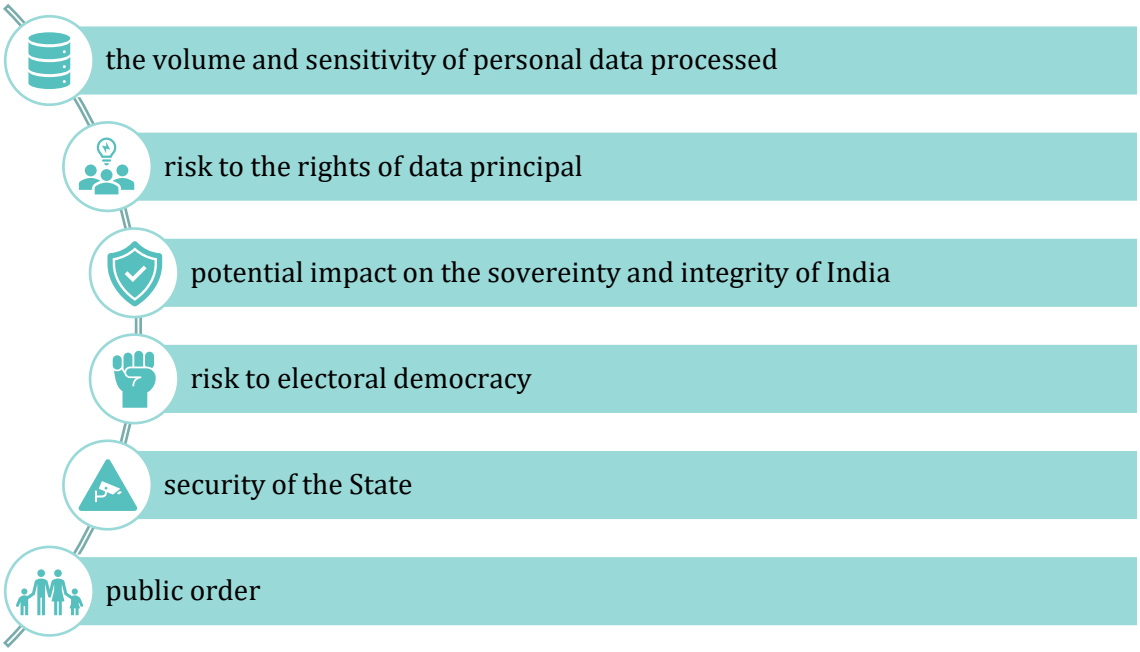
- the data principal withdrawing her consent
- or if the specified purpose for processing the personal data is no longer being served

The personal data can be retained if required for compliance with applicable laws or if the retention obligation is exempt under the provisions of the DPDPA, for example, to enforce a legal claim or a legal right

The specified purpose will be deemed to be no longer served if within a time period, the data principal does not approach the data fiduciary for the purpose or to exercise any of her rights. The time period will be mentioned in the rules.

Who are SDFs?

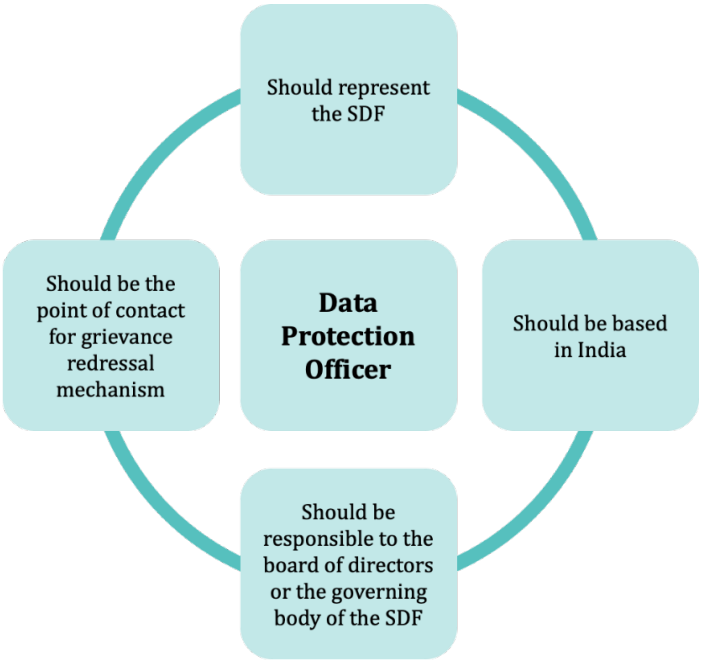
SDF means any data fiduciary or class of data fiduciaries as the Central Government may notify from time to time based on assessment of certain factors that are captured below.



An SDF has certain obligations, in addition to the general obligations of a data fiduciary, listed below:

DPO:

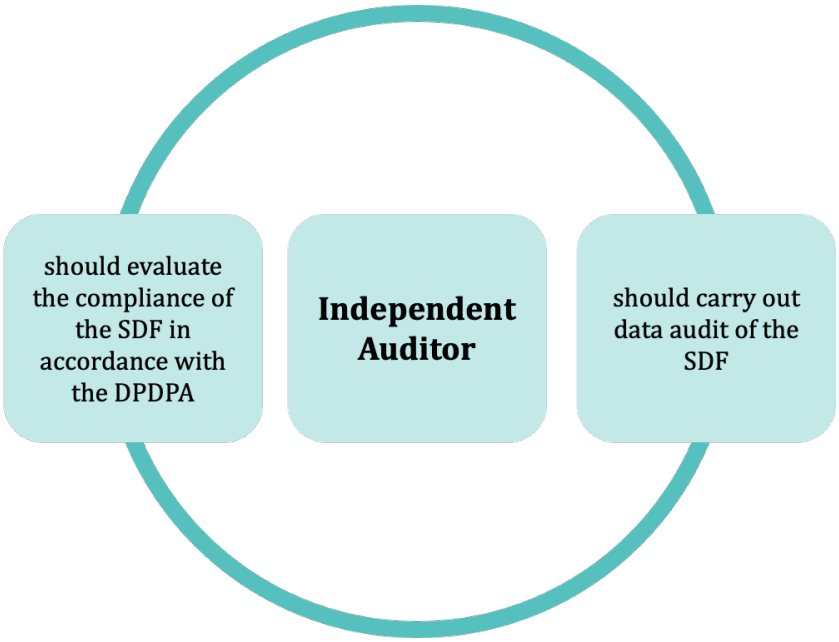
An SDF should appoint a DPO.



Although the DPDPA does not require the appointment of a representative, the SDFs are required to appoint a DPO who is based in India. However, for other data fiduciaries who are not classified as an SDF, there is no requirement to appoint a DPO or representative who is based out of India.

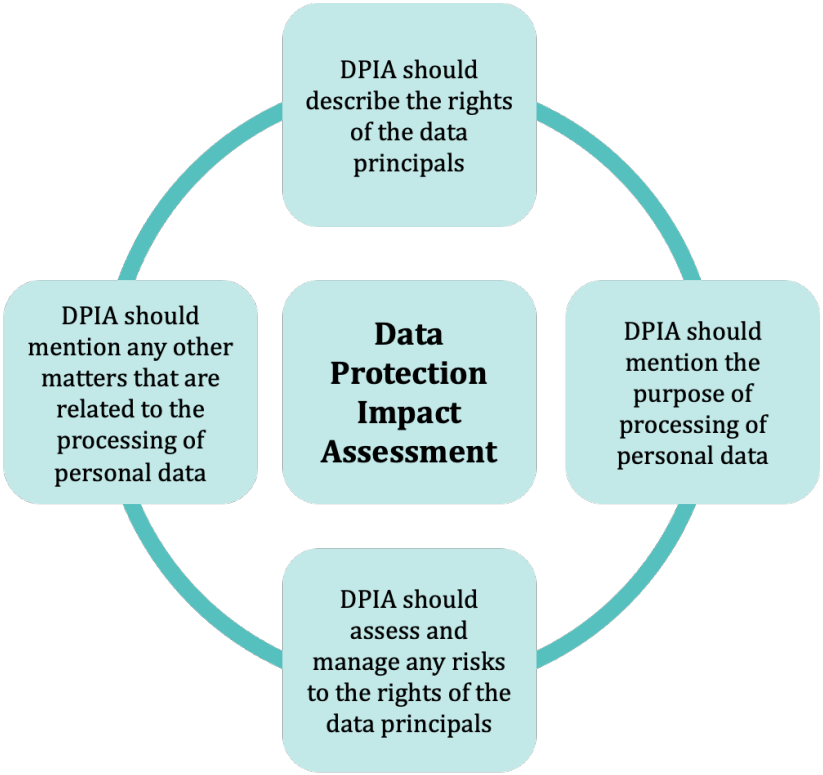
Independent Auditor:

An SDF should appoint an independent auditor.



Data Protection Impact Assessment:

An SDF should undertake periodic Data protection Impact Assessment ("**DPIA**").



The rules will mention the other matters that are related to the processing of personal data that should be part of the DPIA.

Periodic Audit:

An SDF should also undertake periodic audit of its personal data processing activities

Other measures:

An SDF should also undertake other measures that are consistent with the DPDPA. *The rules will mention more measures that an SDF will have to undertake.*

Comparison with select data protection laws around the world

Concept	DPDPA	GDPR	CCPA	PDPA
Implementation of technical and organisational measures	A data fiduciary should implement appropriate technical and organizational measures to comply with DPDPA.	The data controller should implement appropriate technical and organisational measures to comply with GDPR.	A business should implement reasonable security procedures and practices appropriate for the processing of personal information.	An organisation must develop and implement policies and practices to meet the obligations under PDPA.
Appointment of sub-processors	The data fiduciary can appoint a sub-processor through a valid contract.	The controller can appoint processors through a binding written contract.	A business can appoint a service provider for a business purpose pursuant to a business contract.	An organisation can appoint data intermediaries pursuant to a written contract.
Personal Data breach notification	The data fiduciary will notify the board and the affected data principals in case of a personal data breach.	The controller without undue delay and within 72 hours of becoming aware of a personal data breach, notify the supervisory authority and the data subject without undue delay unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.	The California's breach notification statute mandates that consumers should be notified of data breach without unreasonable delay. The business must notify the attorney general if more than 500 consumers' personal information has been breached.	If the data breach is a notifiable data breach, the organisation will have to notify the commission within 3 days from the date of the assessment. The organisation should also notify the affected data subjects.
DPIA	The requirement to undertake a DPIA is only imposed on an SDF.	The controller, prior to the processing, carry out a DPIA where the processing is likely to result in a high risk to the rights and freedoms of natural persons.	Businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security will conduct a risk assessment.	Where an organisation processes personal data based on deemed consent, it will conduct an assessment.
Designation of the DPO	An SDF is obligated to appoint DPO.	The controller may appoint a DPO if its core activities require large-	The CCPA does not obligate the	The organisation must designate an individual to ensure

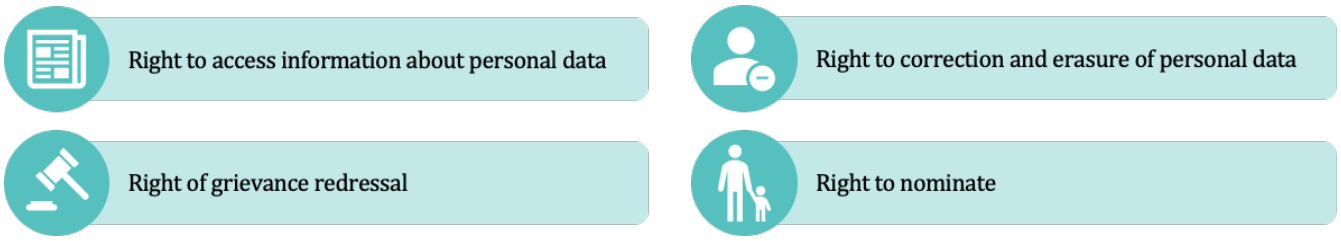
		scale, regular processing and systematic monitoring of individuals or consist of large-scale processing of special categories of data.	appointment of a DPO.	that the organisation complies with the PDPA.
Grievance redressal	Data fiduciaries will establish an effective mechanism to redress the grievances of data principals.	There is no obligation on the controller to provide an internal grievance redressal mechanism under the GDPR.	There is no obligation on the business to provide grievance redressal mechanism under the CCPA.	An organisation should develop a process to receive and respond to complaints that may arise with respect to the application of PDPA.
Retention of personal data	The data fiduciary should erase personal data if the data principal has withdrawn their consent or if the purpose is no longer being served	One of the principles of the GDPR ("storage limitation") mandates that the personal data should not be retained for longer than what is necessary to achieve the purpose of processing.	A business's retention of personal information must be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed.	Organisations should delete personal data as soon as the purpose for which the personal data was collected is no longer being served or if the retention is no longer necessary for legal or business purposes.
Obligation to ensure personal data's completeness, accuracy and consistency	Where the personal data is likely to be used to make a decision that affects the data principal or will be disclosed to another data fiduciary, then the data fiduciary shall ensure its completeness, accuracy and consistency.	One of the principles of data protection is to ensure that the personal data is accurate and, where necessary, kept up to date; if personal data is inaccurate, it should be rectified without delay.	The business has an obligation under the CCPA to entertain consumer requests to correct any inaccuracies in the personal information.	The organisation must take reasonable efforts to ensure that the personal data is accurate and complete where the personal data is likely to be used to make a decision that affects the data subjects or if likely to be disclosed by the organisation to another organisation.
Data audit	DPDPA mandates SDFs to conduct a data audit by an independent auditor.	GDPR does not mandate any data audit by an independent auditor.	CCPA directs the California privacy protection agency to make rules requiring businesses to do annual independent cybersecurity audits if the processing presents significant risk to consumers' privacy or security.	PDPA does not mandate any data audit by an independent auditor.

Rights and duties of data principals under the DPDPA

The crux of the DPDPA is empowering individuals to assert control over their personal data. While the DPDPA is crafted to empower data principals, it also recognizes that individuals hold certain duties to ensure the smooth and responsible processing of their personal data.

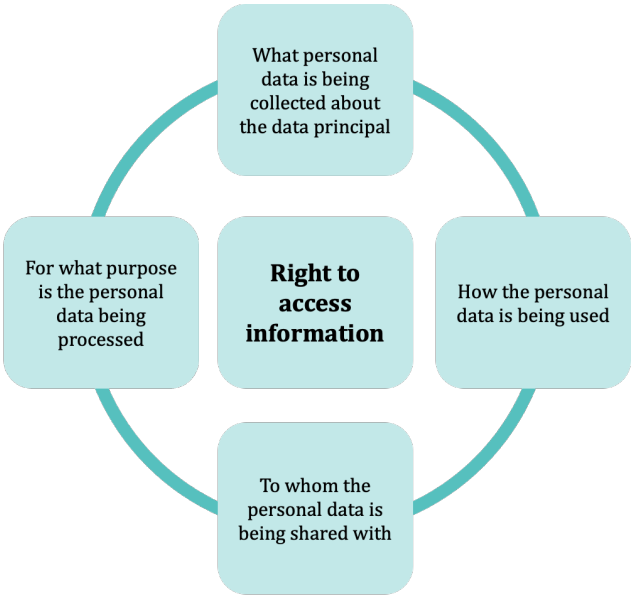
Rights of data principals

DPDPA establishes several key rights for data principals, giving them greater control over how their personal data is processed.



Right to access information:

Data principals have the right to be informed by the data fiduciary, about the purposes for which their data is being processed.



- The right to access information does not extend to the sharing of personal data in response to a request made by a data fiduciary for the purposes of prevention or detection or investigation of offences or cyber incidents, or for prosecution or punishment of offences.
- The right to access information is available only to those who have given consent for the processing of their personal data or volunteered their data.

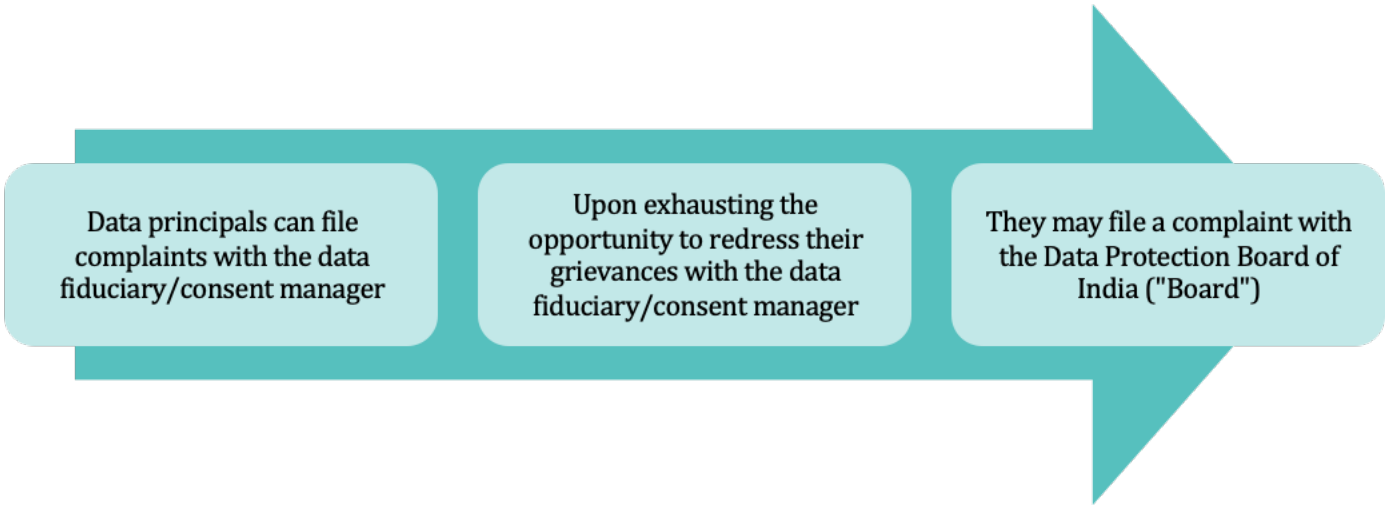
Right to correction and erasure:

DPDPA gives data principals the right to request corrections of any inaccurate or incomplete personal data. This right ensures that personal data remains accurate, relevant, and up to date. If the data is no longer necessary for the purposes for which it was collected, the data principal can request its erasure. Additionally, it is incumbent upon the data fiduciary to inform any associated data processor of such correction or erasure, thereby ensuring that the necessary changes are implemented across the processing chain.

- Unlike GDPR, which establishes a 'right to be forgotten' that allows individuals to request the deletion of personal data made public, compelling data controllers to ensure its removal from public access as well as from third-party entities, such as search engines, DPDPA does not explicitly provide for this right.
- The right to correction and erasure of personal data is available only to those who have given consent for the processing of their personal data or volunteered their data.
- The rules will prescribe the manner in which the data principal will make their request to the data fiduciary for erasure of their personal data.
- Fulfilling the right to correct or erase personal data requires the data principal to submit verifiable information. This protects against fraudulent changes and ensures the accuracy of the data retained by fiduciaries.
- While the data principal has several rights under DPDPA, exercising these rights must be done in accordance with existing laws. For instance, the data principal cannot ask for the erasure of data that a company is legally required to retain, such as for compliance with tax regulations or other statutory obligations.

Right to grievance redressal:

DPDPA empowers data principals to have recourse to a mechanism to address any grievances related to data processing.



- The Board, as defined in DPDPA, will be an independent regulatory authority established to oversee the implementation of data protection laws in India. It will be responsible for addressing complaints, adjudicating disputes, and ensuring compliance with the DPDPA's provisions.
- The rules will prescribe the time period within which the data fiduciary or consent manager would need to respond to any grievances.

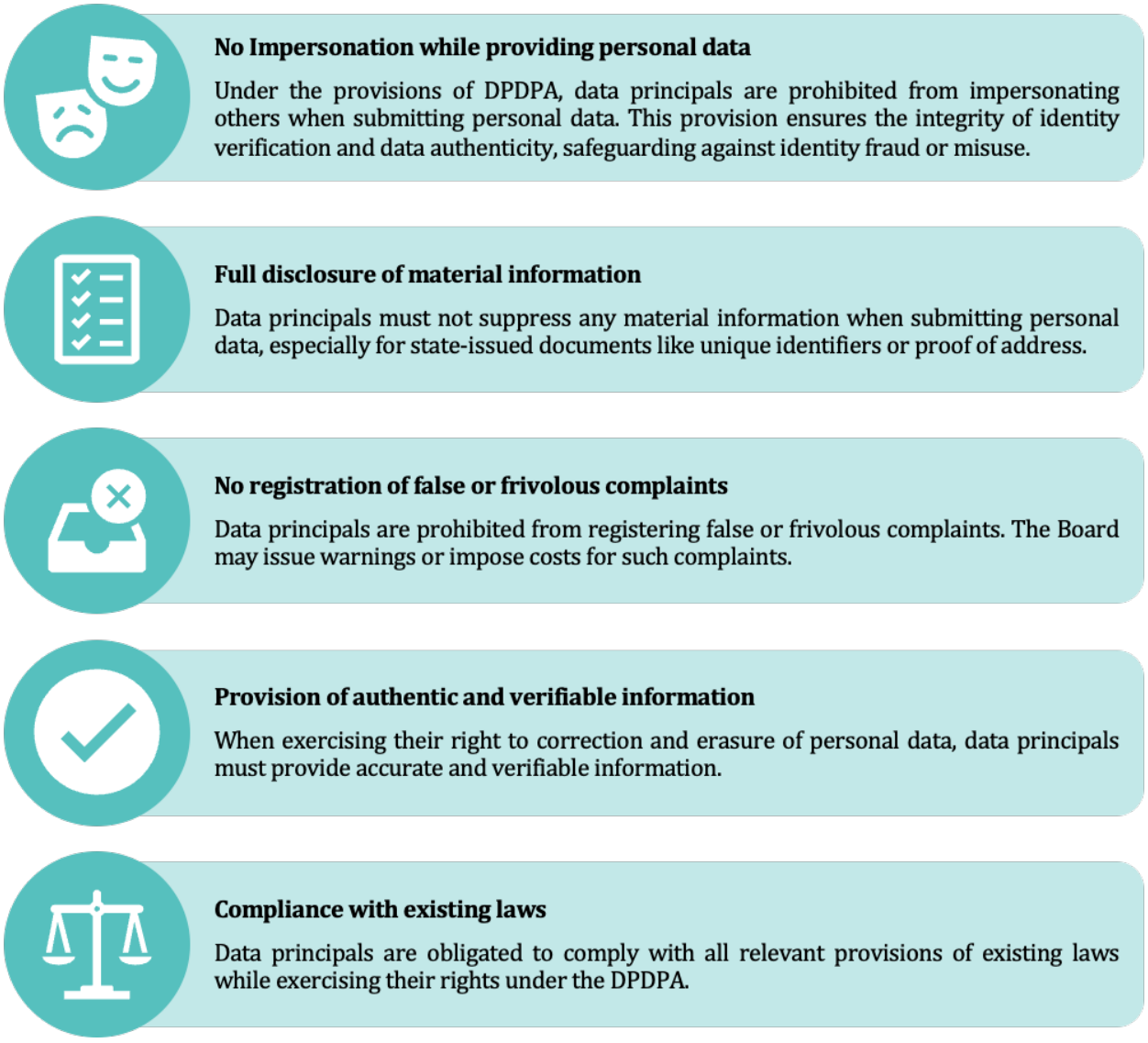
Right to nominate:

DPDPA allows a data principal to nominate another person to exercise their rights in case of death or incapacity. This ensures continuity in protecting personal data even when a data principal is no longer able to do so.

- The expression '*incapacity*' means inability to exercise the rights of the data principal under the provisions of DPDPA or the rules made thereunder due to unsoundness of mind or infirmity of body.
- The manner in which the data principal will nominate any other individual will be prescribed by the rules.

Duties of data principals: responsibility matters

The DPDPA recognizes the importance of preventing frivolous complaints by data principals. To achieve this, data principals are assigned specific duties that ensure responsible use of their rights within the data processing framework.



In order to secure the right to fair grievance redressal, the duty of the data principal is to submit only legitimate complaints. Misuse of the system by filing false complaints can result in warnings or penalties from the Board.

Comparison with Global Data Protection Laws

The rights and duties of data principals under DPDPA align with global data protection standards but feature some differences in scope and application. Here's a comparative analysis with the GDPR (EU), CCPA (California), and PDPA (Singapore):

Concept	DPDPA	GDPR	CCPA	PDPA
Right to access information about personal data	Data principals have the right to access their personal data, processing purposes, and details of entities with whom data is shared.	Data subjects have the right to access their personal data, the purposes of processing, and any recipients of the data.	Consumers can request access to the categories and specific pieces of personal information collected.	Individuals have the right to request access to their personal data held by organizations, including processing purposes.
Right to correction and erasure of personal data	Individuals have the right to correction, completion, updating and erasure of their personal data for processing, the consent for which is previously given.	Data subjects have the right to rectify inaccurate data and request erasure under specific conditions for example, where the personal data is no longer necessary, or the data subject withdraws consent or objects to the processing.	Consumers can request the correction of inaccurate data and the deletion of personal data under certain conditions for example, when the transaction for which data was collected has lapsed, or where there is a legal obligation to delete the data.	Individuals have the right to request the correction of inaccurate data and the deletion of data when it is no longer necessary.
Right of grievance redressal	Data principals can file complaints with the grievance officer and upon exhaustion, approach the data protection officer in case of violations of their rights.	Data subjects can lodge complaints with the supervisory authority, specifically the member state of their residence, if their rights have been violated. They may also seek private remedies through the courts.	Consumers have the right to seek grievance redressal through the California attorney general for violations of their privacy rights, and they can also bring civil actions in case of data security breaches that violate their rights.	Individuals can file complaints with the personal data protection commission for violations of their rights.
Right to nominate	Data principals can nominate another person to exercise the rights in case of incapacity or death.	Data subjects can appoint a representative to exercise the rights on their behalf.	No direct provision for nominating a representative to exercise rights in the event of incapacity or death.	No specific provision for nomination, though rights can generally be exercised by legal guardians or representatives.
Other rights	No explicit provisions for: • data portability; • objection to automated processing and profiling;	Also includes rights to: • data portability; • object to automated individual decision making, including profiling and	Consumers can: • Opt-out of data sales; and • Request data in a portable format.	Includes rights to: • Data portability; • Objection to processing; and • Restriction of processing when

Concept	DPDPA	GDPR	CCPA	PDPA
	• restriction of processing; and • right to be forgotten.	processing for direct marketing; • restriction of processing; and • be forgotten.		consent is withdrawn.
Duties of the data principal	• Refrain from impersonating other individuals. • Ensure full disclosure of material information. • Avoid filing false or frivolous complaints. • Provide accurate and verifiable information. • Comply with all applicable laws.	• Provide accurate and up to date data information. • Provide necessary verifiable information when making data access or rectification request. • Provide information without causing undue delays. • Refrain from making unfounded or excessive requests when exercising rights.	• Provide accurate and truthful information. • Refrain from making excessive requests for access or deletion. • Verify the identity before submitting requests for access or deletion.	• Provide accurate and complete personal data. • Avoid making frivolous or vexatious access or correction requests. • Comply with legal obligations when exercising right to access or correct personal data.

International transfer of personal data

Restriction on transfer of personal data in the DPDPA

The Central Government, by notifications ▶ may restrict the transfer of personal data by a data fiduciary for processing to a country or territory outside India.

- The transfer of personal data can be restricted to countries or certain territories.
- Unlike the GDPR which allows for implementing appropriate safeguards (*like incorporating standard contractual clauses, or binding corporate rules*), or permits relying on derogations (*such as relying on data subject's consent*) for cross-border transfer of personal data, DPDPA does not allow alternative transfer mechanisms to undertake transfer of personal data outside India.
- In the SPDI Rules, a body corporate or its processors could transfer sensitive personal data to any body corporate located in any other country that ensures the same level of data protection as provided under the IT Rules for the performance of a lawful contract between the body corporate or its processors and the data subject or if the data subject has consented to such data transfer.

Applicability of other laws

If there are any laws that provide for a higher degree of protection or a higher restriction on transfer of personal data by a data fiduciary or significant data fiduciary ▶ Then the DPDPA will not restrict the applicability of such laws.

1. There are various sectoral regulations that mandate the storage of data within the boundaries of India, for example; the Reserve Bank of India's ("**RBI**") circular No. 2785/06.08.005/2017-18 dated April 6, 2018 mandates entities in the payment ecosystem to store payment systems data in India; the Companies Act of 2013 mandates companies to maintain books of account in electronic mode in India, and registers and copies of the annual return filed to be kept at the registered office of the company; companies providing voice based business process outsourcing services (which are called as '*Other Service Providers*' ("**OSPs**")) are required to maintain a copy of certain data and system logs in India if their Electronic Private Automatic Branch Exchange (EPABX) is outside in India as per the revised OSP guidelines No. 18-8/2020 dated June 23, 2021 released by the Department of Telecommunications, etc.
2. Territorial blacklists are not uncommon and are also seen in some other laws in India. For example, under the extant foreign exchange laws in India, a person cannot acquire/transfer any immovable property in India, other than lease, not exceeding 5 (five) years without permission from RBI if they belong to any of the following countries: Pakistan, Bangladesh, Sri Lanka, Afghanistan, China, Iran, Nepal, Bhutan, Macau, Hong Kong, Democratic People's Republic of Korea. Similarly, the Export Credit Guarantee Corporation of India ("**ECGC**") has classified certain countries like Afghanistan, Sri Lanka, Syria, Central African Republican, Ghana, North Korea, Palestine, Zimbabwe, etc. as restricted countries since they pose high political risks. The export of goods to such countries requires the prior approval of the ECGC.

Comparison with select data protection laws around the world

DPDPA	GDPR	CCPA	PDPA
Under DPDPA, the Central Government may release a list of countries or territories to which personal data may not be transferred. Any applicable law that provides for a higher degree protection of personal data or higher restriction on transfer of personal data will supersede the provisions of DPDPA.	The GDPR permits the cross-border transfer of personal data based on an adequacy decision. In the absence of such a decision, transfers may occur by implementing appropriate safeguards, which may include the use of standard contractual clauses or binding corporate rules. If neither an adequacy decision nor appropriate safeguards are in place, the GDPR allows for the transfer of personal data under specific derogations. These derogations include situations where the data subject has given explicit consent, where the transfer is necessary for the performance of a contract, or where it serves a legitimate public interest. Transfers may also be conducted if they are necessary for the establishment, exercise, or defence of legal claims, among other valid grounds.	The CCPA does not specifically mention any restriction on international transfer of personal data.	An organisation may transfer personal data to a country or territory outside of Singapore, provided that the organisation ensures a standard of protection for the personal data transferred as provided under the PDPA. The Personal Data Protection Commission may exempt organisations from the above requirement.

Specific processing and general exemptions under the DPDPA

Specific processing: Data relating to children and persons with disabilities

DPDPA lays out specific guidelines for the processing of personal data related to children and individuals with disabilities, who are under the care of a lawful guardian. These provisions emphasise the protection of vulnerable groups from potential misuse of their data.

Verifiable consent requirement:

Before processing any personal data of a child (below 18 (eighteen) years of age) or of a person with disability under a lawful guardian, verifiable consent of the parent or guardian must be obtained. This ensures that only authorised adults may give permission for data processing in these cases, thereby safeguarding the privacy of children and vulnerable individuals.

- The expression, 'consent of the parent' includes the consent of lawful guardian, wherever applicable.
- The Rights of Persons with Disabilities Act, 2016 defines 'Person with disability' as a person with long term physical, mental, intellectual or sensory impairment which, in interaction with barriers, hinders his full and effective participation in society equally with others.

Protection of well-being:

Data fiduciaries are expressly forbidden from processing personal data in a manner that could have a detrimental effect on the well-being of the child. This clause prioritises the physical and mental welfare of minors, ensuring that harmful data practices do not negatively impact them.

Prohibition on tracking, monitoring, and targeted advertising:

Data fiduciaries are prohibited from tracking, conducting behavioural monitoring, or serving targeted advertising towards children. This addresses concerns about digital surveillance and manipulative advertising that can exploit children's vulnerable and impressionable mind.

- Digital surveillance involves the tracking of users' online activities to gather personal data, often without explicit consent, while manipulative advertising uses this data to influence consumer behavior in subtle or exploitative ways.
- Tracking refers to the practice of collecting information about users' activities across websites, apps, or online services over time. This can include details like browsing history, location, and interactions, often done through cookies or other tracking technologies.

- Behavioral monitoring involves analysing the patterns of a user's behavior such as their clicks, searches, or time spent on certain content to build a profile or predict future actions. For children, this can raise privacy concerns, as it allows for detailed surveillance of their online habits.
- Targeted advertising uses collected data to deliver advertisements specifically tailored to an individual's preference or behavior. When applied to children, this can be manipulative, as it takes advantage of their undeveloped ability to critically assess marketing tactics, increasing the risk of exploitation.

Exemptions for specific classes of data fiduciaries for processing data of a child or individuals with disability:

The Central Government has the authority to exempt certain classes of data fiduciaries from adhering to the provisions regarding obtaining verifiable consent and avoiding tracking or targeted advertising. These exemptions would be made only under prescribed conditions or for specific purposes, ensuring flexibility for legitimate processing needs, while still protecting children's rights.

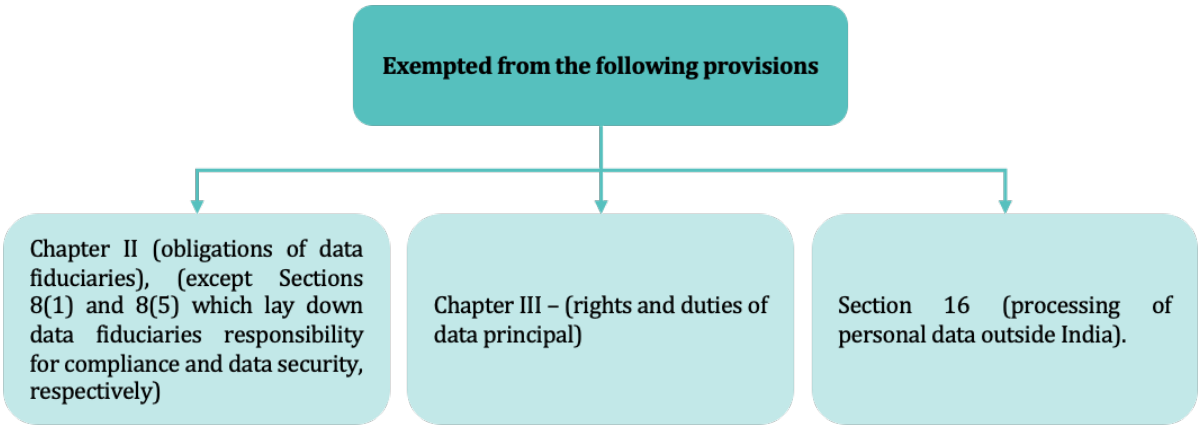
Age-based exemptions for safe processing:

If a data fiduciary demonstrates that its data processing practices regarding children's data are verifiably safe, the Central Government may permit the data fiduciary to process data of individuals above a specific age without the necessity of obtaining consent or avoiding tracking.

General exemptions

Exemptions applicable to certain types of data processing

DPDPA provides for exemptions where certain data processing requirements do not apply.



Section 17 of DPDPA states that the provisions of the Act mentioned above do not apply under certain conditions. Here is a detailed breakdown of the processing activities that are exempted from the above provisions:

Legal and judicial exemptions:

DPDPA provides the exemptions listed above for processing in circumstances where it is necessary for enforcing any legal right or claim. Additionally, personal data processing by any court, tribunal, or regulatory body that is entrusted by law with performing judicial, quasi-judicial, or supervisory functions is exempted. This ensures that these bodies can perform their functions effectively.

Prevention, detection, and investigation of offences:

DPDPA allows exemptions listed above for data processing that is necessary for the prevention, detection, investigation, or prosecution of offences or contraventions of laws in India. This exemption is crucial for law

enforcement agencies to carry out their duties efficiently without needing to navigate through consent-based data processing regulations, which may otherwise delay the timely investigation and prosecution of crimes.

Corporate restructuring:

DPDPA allows exemptions from data processing necessary for corporate restructuring activities, including mergers, amalgamations, demergers, and other forms of restructuring approved by courts or competent authorities. These processes often involve large volumes of sensitive data, and DPDPA recognises the practical necessity of processing this data without restrictive consent obligations.

Outsourcing contracts:

DPDPA states that the processing of personal data of data principals who are not within the territory of India is exempted from the above-mentioned provisions, as long as the processing is conducted pursuant to a contract with a foreign entity.

This provision stipulates that when an Indian entity processes the personal data of individuals located outside India under a contract with someone outside India, it must comply only with Sections 8(1) and (5). Essentially, this means that, irrespective of any agreement to the contrary, the fiduciary must ensure compliance with the Act for any processing, including that performed by a data processor on its behalf (as per Section 8(1)), and must take reasonable security safeguards to prevent data breaches (as required by Section 8(5)).

Loan defaults:

Exemptions are also provided when personal data is processed to ascertain the financial information and assets and liabilities of a person who has defaulted on loans or advances from financial institutions. This provision aligns with the Insolvency and Bankruptcy Code, 2016 and enables financial institutions to assess the financial status of defaulters. In such cases, stringent data processing requirements are relaxed, allowing financial institutions to take necessary action for recovery of dues.

- For the purposes of this clause, the expressions ‘default’ and ‘financial institution’ will have the meaning respectively assigned to them in sub-sections (12) and (14) of Section 3 of the Insolvency and Bankruptcy Code, 2016.
- ‘Default’ means, non-payment of debt when whole or any part or instalment of the amount of debt has become due and payable and is not repaid by the debtor.
- ‘Financial Institution’ means a schedule bank, financial institution as defined by the RBI Act, 1934, public financial institutions defined by the Companies Act, 2013 and such other institutions as the central government may by notification specify as financial institution.

Exemption for Research, archiving, and statistical purposes:

Personal data processing for research, archiving, or statistical purposes is also exempt from the provisions of the DPDPA, provided that the data is not used to make decisions specific to any individual and complies with prescribed standards. This provision acknowledges the importance of data for academic and policy-making endeavours, facilitating research without imposing excessive data protection barriers.

Exemptions by class of fiduciaries:

DPDPA provides exemptions for specific classes of fiduciaries, including startups and state entities. These exemptions reduce compliance burdens for certain organisations while maintaining core data protection standards.

Startups:

DPDPA empowers the Central Government to declare that specific provisions of the DPDPA will not apply to certain classes of data fiduciaries for a specified period. This power enables the Government to exempt certain entities from the provisions of DPDPA based on the volume and nature of the personal data they process. This includes startups, which may be given exemptions from Section 5 (*notice for data processing*), Section 8(3) and (7) (*data accuracy and erasure*), Sections 10 and 11 (*significant fiduciary obligations and right to access information*), to promote innovation and growth in their early stages.

This approach fosters a favourable environment for startups while ensuring that they remain compliant with the broader objectives of the DPDPA. Startups can thereby operate with reduced regulatory burden during their initial growth phases, encouraging innovation while gradually moving toward full compliance as they scale.

A '**startup'** refers to a private limited company, partnership firm, or limited liability partnership established in India that is not older than 10 (ten) years, has an annual turnover of less than INR 100,00,00,000 (Indian Rupees one hundred crore), and is focused on innovation or scalable business models. It must also receive recognition under the guidelines defined by the Department for Promotion of Industry and Internal Trade.

State entities:

States or any instrumentalities of the State, are provided exemptions from provisions of Section 8(7) (*erasure*) and Section 12(3) (*right to erasure*) of the DPDPA. and, where such processing is for a purpose that does not include making of a decision that affects the data principal, Section 12(2) (*right to correction*) is also exempted. This ensures that administrative functions of the State are carried out efficiently without violating privacy standards.

DPDPA exempts processing by States or any instrumentalities of the State notified by the Central Government from the provisions of the DPDPA when such processing is essential for the sovereignty and integrity of India, national security, friendly relations with foreign nations, maintenance of public order, or preventing incitement to cognizable offenses.

- The Central Government may, within 5 (five) years of the commencement of DPDPA, issue a notification to exempt certain provisions of DPDPA from applying to specified data fiduciaries or classes of data fiduciaries for a designated period.
- Moreover, the DPDPA also recognises that the States or any instrumentalities of the State often need to process personal data for the delivery of services and benefits to citizens. Under the DPDPA, a data fiduciary may process the personal data of a data principal when the State is providing subsidies, benefits, services, certificates, licenses, or permits. For instance, when an individual consents to provide data for maternity benefits, as is illustrated in Section 7(b) of DPDPA, the Government can continue to use this data for other related services, such as health or social benefits, without needing fresh consent each time. This provision allows government welfare programs to function without unnecessary administrative hurdles, ensuring that personal data already collected can be utilised across different services efficiently. In essence, this provision compliments the exemptions under DPDPA by enabling smoother governmental operations where data is already consented for or maintained by state bodies.

Comparison with Global Data Protection Laws

The special provisions and exemptions under the DPDPA align with international data protection laws on certain aspects and exhibit differences in others. Below is a comparative analysis of these provisions alongside the GDPR (EU), CCPA (California), and PDPA (Singapore):

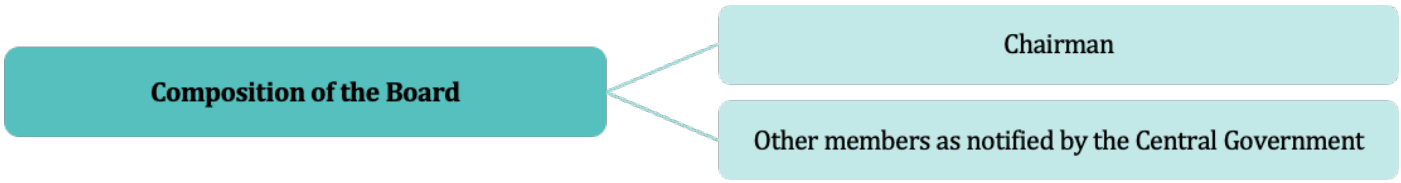
Concept	DPDPA	GDPR	CCPA	PDPA
Legal rights or claims	Provides for an exemption when processing is necessary to enforce a legal right or claim.	Retaining data for the purpose of the establishment, exercise, or defence of legal claims, or for compliance with legal obligations, is exempt from the right to erasure, right to restriction of processing, and other such rights of the data subject.	Exempts personal data processing for compliance with legal obligations from the CCPA's provisions on the right to deletion.	PDPA does not affect any authority, right, privilege or immunity conferred, or obligation or limitation imposed, by or under the law, including legal privilege.
Law enforcement and crime prevention	Provides an exemption for the processing of personal data for the purposes of, preventing, detecting, investigating, or prosecuting violations of law.	Allows for the processing of personal data relating to prevention and detection of crime, convictions and offences or related security measures, but only under the control of official authority or when authorised by union or member state law providing for appropriate safeguards for the rights and freedom of data subjects as provided under EU law enforcement directive.	No specific exemption provided for.	No specific exemption provided for.
Corporate restructuring	Exempts processing when it is required for the legal approval of the company mergers, acquisitions, demergers, or restructuring by a court or relevant authority.	No specific mention of corporate restructuring being exempted.	Sale or merger triggers consumer rights if the third party materially alters personal information during the course of such transaction; however, there is no mention of such transactions being exempted from certain provisions relating to data processing.	No specific mention of corporate restructuring as an exemption.

Concept	DPDPA	GDPR	CCPA	PDPA
Loan defaults	Provides for exemption to processing when the purpose is for ascertaining financial information and assets and liabilities of any person who has defaulted in payment due on account of a loan or advance taken from a financial institution.	There is no specific mention that loan defaults or the collection of financial information are exempted.	There is no specific mention that loan defaults or the collection of financial information are exempted.	There is no specific mention that loan defaults or the collection of financial information are exempted.
Startups and State entities	Exempts certain startups from specific provisions as notified by the Central Government, based on the volume and nature of data processed.	No specific exemption for startups or state entities.	No specific exemption for startups or state entities.	No specific exemption for startups or state entities.
Children's data protection	Verifiable parental consent required for children under 18 (eighteen) years; no tracking or behavioural monitoring. DPDPA further prohibits tracking/targeted advertising for children	Where the child is below the age of 16 (sixteen) years, processing will be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.	While the CCPA doesn't have special provisions for children's data, COPPA (Children's Online Privacy Protection Act of 1998) does require verifiable parental consent before collecting, using, or disclosing personal information from children under the age of 13 (thirteen) years.	PDPC states that children aged between 13 (thirteen) and 17 (seventeen) years are allowed to give valid consent if the data policies are clear and understandable to them, including the consequences of providing and withdrawing consent. However, if the organisation believes the child lacks sufficient understanding, consent should be obtained from the child's parent or guardian.

Enforcement and penalties under the DPDPA

Board

The Board under DPDPA, will be an independent corporate entity empowered to enforce the DPDPA, adjudicate on complaints related to data protection violations, impose penalties, and provide guidance on the implementation of data protection laws.



The Board members serve renewable 2 (two) year terms, and post-tenure employment with any data fiduciaries previously overseen is restricted to avoid conflicts of interest. The chairperson holds administrative authority, including assigning responsibilities, managing administrative matters, and delegating functions among members. In the chairperson's absence, the senior-most member assumes these duties.

The members, officers, and employees of the Board are classified as public servants under the Bharatiya Nyaya Sanhita, 2023, which subjects them to specific accountability standards while discharging their regulatory duties. Its core responsibilities include:

Response to personal data breaches:

remedial and mitigation measures: On receiving notification of a personal data breach, the Board is empowered to direct urgent remedial or mitigation measures to address the breach immediately. Following this, the Board may conduct an inquiry into the breach and, if warranted, impose penalties.

Handling complaints and references:

1. Data principal complaints: If a data principal submits a complaint about a personal data breach, or a failure by a data fiduciary to meet its obligations, the Board is authorised to conduct an inquiry and, where appropriate, impose penalties.
2. Consent manager complaints: The Board may also inquire into and penalise any breach by a consent manager regarding its obligations towards a data principal's personal data.
3. Breach of registration conditions: In the event of a breach of any registration condition by a consent manager, the Board has the authority to investigate and impose penalties as it is vested with the powers of a civil court.
4. Intermediary breaches: The Board may investigate breaches of Section 37 (2) (*Power of Central Government to issue directions*) by an intermediary based on a reference from the Central Government and impose penalties as stipulated in DPDPA.

Issuance and modification of directions; directive powers:

For effective enforcement, the Board may issue directions necessary for compliance. These directions are binding, and the Board must provide an opportunity for the concerned party to be heard, along with documented reasons for the directive.

Upon receiving a representation from an affected party or a referral from the Central Government, the Board holds the power to modify, suspend, withdraw, or cancel issued directions. In doing so, the Board can impose conditions it deems appropriate, specifying the terms under which the modification or cancellation is effective.

This consolidated framework establishes the Board as a pivotal entity in the enforcement of data protection compliance, enabling prompt responses to breaches, robust oversight of obligations, and clear mechanisms for modifying and enforcing compliance directives.

Complaints and Resolution

The procedural framework of the Board is structured to allow for systematic handling of data breaches and complaints. Below is a step-by-step breakdown:

Complaint and reference review

Upon receiving a complaint, government reference, or court directive, the Board examines its validity. If grounds are determined insufficient, the case may be closed with reasons recorded in writing.

Grounds for inquiry determination

When grounds are sufficient, the Board decides whether an inquiry is warranted. The Board is empowered to examine the activities of any entity suspected of violating DPDPA provisions.

Issuance of interim orders

If immediate action is necessary, the Board can issue interim orders to prevent or mitigate further breaches, following a fair hearing for the affected party.

Final decision and documentation

Upon concluding the inquiry, the Board may either close the case or impose penalties and sanctions as outlined in DPDPA, ensuring that all decisions are substantiated with written documentation.

Appeals to Appelate Tribunal

Individuals aggrieved by an order from the Board may appeal to the Appellate Tribunal within 60 (sixty) days of receiving the order. The Appellate Tribunal can allow late appeals for valid reasons. After reviewing the case and hearing from all the parties, it can confirm, modify, or overturn the Board's order. If any party is not satisfied with the decision of the Appellate Tribunal, they may futher appeal to the Supreme Court.

Additional factors:

1. The Board functions as a digital office, managing the receipt, hearing, and resolution of complaints entirely online, implementing techno-legal measures as necessary.
2. During the inquiry, the Board abides by principles of natural justice, meticulously documenting each action taken to ensure transparency.
3. To effectively discharge its responsibilities, the Board is vested with the powers of a civil court**.** Additionally, the Board has the authority to inspect relevant documents and records.
4. The Board avoids impeding daily business activities, refraining from seizing premises or equipment essential for operations during inquiries.
5. The Board may request assistance from police or government officers to carry out its investigations, and such officers are legally obliged to comply.
6. To discourage abuse of the complaint process, the Board may issue warnings or impose costs on complainants if a complaint is deemed false or frivolous.
7. "Appellate Tribunal" means the Telecom Disputes Settlement and Appellate Tribunal established under Section 14 of the Telecom Regulatory Authority of India Act, 1997.

Alternative Mechanisms

Mediation:

The Board may recommend mediation if it believes a complaint can be resolved amicably. Parties are encouraged to engage with mutually agreed mediators or follow relevant Indian mediation laws, promoting collaborative solutions to disputes.

Mediation is an Alternative dispute resolution ("**ADR**") process where a neutral third party, known as a mediator, assists the disputing parties in reaching a mutually acceptable agreement. The mediator does not make a decision but facilitates communication, helping parties find common ground and solutions voluntarily. The Code of Civil Procedure, 1908 allow courts to refer cases for mediation when they see the potential for an amicable settlement. Since the Board is vested with powers similar to that of civil courts, the Board may also refer cases to mediation where it deems fit.

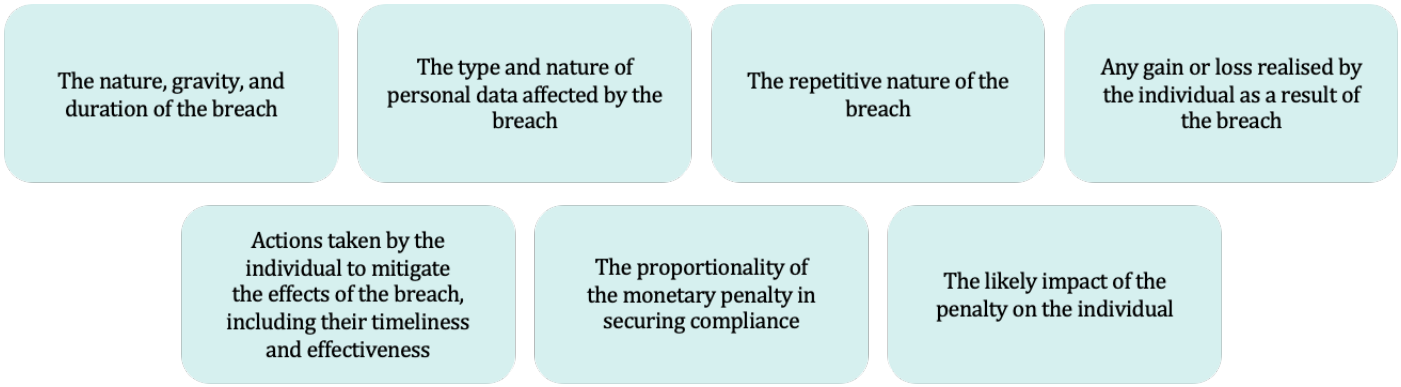
Voluntary Undertakings:

The Board can accept voluntary undertakings from individuals to ensure compliance with the DPDPA at any stage of a proceeding. These undertakings may include commitments to take specific actions or refrain from certain behaviours. The Board can modify the terms with mutual consent. While a voluntary undertaking can halt further proceedings on the related issues, failure to comply is treated as a breach of DPDPA, allowing the Board to initiate enforcement actions after giving the individual a chance to be heard. This process fosters compliance and accountability among stakeholders.

Penalties under DPDPA

Under the DPDPA, if the Board determines that a significant breach of DPDPA or its rules has occurred, it may impose a monetary penalty after providing the individual with an opportunity to be heard. In assessing the appropriate penalty, the Board considers several factors to ensure that penalties are proportional and effective in deterring future violations.

These factors include:



The penalties for specific breaches are as follows:

Breach of provisions of the DPDPA or rules made thereunder	Penalty
Breach of security safeguards under Section 8(5)	Up to INR 250,00,00,000
Failure to notify the Board or affected data principal of a breach under Section 8(6)	Up to INR 200,00,00,000
Breach of obligations concerning children under Section 9	Up to INR 200,00,00,000
Breach of obligations for SDFs under Section 10	Up to INR 150,00,00,000
Breach of duties of data principal under Section 15	Up to INR 10,000
Breach of voluntary undertakings accepted by the Board under Section 32	Penalties vary based on the breach
Any other violations of the DPDPA or its rules	Up to INR 50,00,00,000

Under Section 37 of the DPDPA, the Central Government is empowered to block public access to information held by a Data Fiduciary that has been subject to monetary penalties for violations of data protection regulations, in 2 (two) or more instances. This action is initiated upon a formal recommendation from the Board. Importantly, the data fiduciary is afforded an opportunity to respond before any blocking order is issued, ensuring a degree of procedural fairness. Compliance with such directives is mandatory for intermediaries, with terms clearly defined in alignment with the Information Technology Act, 2000, highlighting the intersection of data protection and regulatory enforcement.

All sums collected as penalties will be credited to the Consolidated Fund of India.

The Consolidated Fund of India is the main fund of the Indian Government, where all revenues received (like taxes), loans raised, and money received in repayment of loans are deposited. It's essentially the government's primary financial reservoir, set up under Article 266(1) of the Indian Constitution.

Comparison with Global Data Protection Laws

The table below compares enforcement and penalty provisions across the DPDPA, GDPR, CCPA, and PDPA, highlighting key differences in penalty scope, criteria for fines, appeal mechanisms, and revenue allocation.

CONCEPT	DPDPA	GDPR	CCPA	PDPA
Enforcement body	Board	Data Protection Authorities in each EU member State (supervisory authorities)	Direct CCPA/ (California Consumer Privacy Act) issues will be referred to the California Privacy Protection Agency as the main enforcement authority. The California Attorney General's office is involved mainly in data breach consumer suits or significant oversight cases	Personal Data Protection Commission
Maximum penalty amount	Up to INR 250,00,00,000 for security breaches, unauthorised processing, and non-compliance (per the DPDPA's Schedule)	Up to Euro 20,000,000 or 4% of global annual turnover, whichever is higher	Fines up to USD 7,500 per intentional violation and USD 2,500 per unintentional violation	Up to SGD1,000,000 for each breach
Appeal process	Appeals against Board's decisions can be made to the Appellate Tribunal, with further appeal options under the Telecom Regulatory Authority of India Act, 1997 for unresolved cases	Right to judicial appeal against penalties before national courts	No specific provision mentioning the appeal process.	Appeals against penalties may be submitted to the Data Protection Appeal Committee
ADR	The Board may recommend mediation for complaints that may be resolved without further litigation	ADR mechanisms available at the discretion of national supervisory authorities	Does not specify ADR mechanisms directly within its provisions	No specific ADR; enforcement handled by the Personal Data Protection Commission

Processing of employees' personal data

Transition from the SPDI Rules to the DPDPA

The transition to the DPDPA marks a significant shift from the previous SPDI Rules, bringing a more rigorous data protection framework that requires employers to update their data management practices. Employers will need to revise internal data protection policies to align with the DPDPA, especially in areas such as employee rights and data breach management. As the SPDI Rules phase out, employers should also prepare for mandatory reporting of data breaches and ensure that internal response protocols are aligned with the DPDPA's requirements.

Roles under the DPDPA

Employer: The employer will be considered as a '*data fiduciary*'.

Employee: The employee will be considered as a '*data principal*'.

Third Parties: The third parties processing data on behalf of the employers, will be a '*data processor*'.

For example: human resources, management software

Legal basis for processing the personal data of employees under the DPDPA

The DPDPA provides certain legitimate uses under which the processing of personal data can be undertaken, without consent. One of the legitimate uses is processing personal data for the purposes of employment.

The data fiduciary can process the personal data of a data principal for:

'the purposes of employment'

or *'those related to safeguarding the employer from loss or liability such as corporate espionage'*,

'for maintenance of confidentiality of trade secrets, intellectual property, classified information'

or *'for provision of any service or benefit sought by a data principal who is an employee'*

1. It remains to be seen if, in line with international laws, the scope of 'purposes for employment' under the DPDPA include processing of personal data both before and after employment. This interpretation would encompass activities such as background verification prior to employment, as well as retaining employment records post-tenure for compliance with applicable laws.
2. The processing of personal data for service or benefit sought by a data principal may include employee training programs, employee stock option plans, medical facilities, etc.

Legal basis for processing personal data of data principals who are not considered to be 'employees'

The DPDPA does not define 'employees', creating uncertainty about the applicability of the law to other individuals working for an organisation, such as independent contractors, freelancers, consultants, temporary/part-time workers, interns, and apprentices. In the absence of a clear definition, some parallels can be drawn to interpretations in other

data protection laws, where the concept of 'employment' is often understood to extend beyond traditional employment relationships. For example, some global laws treat individuals working under contractual arrangements, such as freelancers and consultants, similarly to employees when processing personal data for work-related purposes. This broad interpretation of 'employment' could influence the scope of data processing obligations under the DPDPA, even if no direct guidance is provided in the Indian context.

Relying on 'consent' to process the personal data of the above-mentioned individuals may not be meaningful since the individuals may not be able to provide 'free', and 'unconditional' consent due to the nature of the relationship between the individual and the data fiduciary.

Key considerations for employers under the DPDPA

Employer obligations under the DPDPA

Under the DPDPA, employers must adhere to several key obligations to ensure responsible data handling and protect employee personal data. First, they are required to assess processors who may be processing employee data for the DPDPA compliance before engagement and enter into a valid written contract to formalise these arrangements. Employers must also establish an internal mechanism that allows employees to exercise their rights under the DPDPA, including a grievance system to resolve concerns effectively. Additionally, implementing appropriate technical, organisational, and reasonable security measures is essential to prevent data breaches, along with a mechanism to promptly inform employees in case of such breaches. For employers classified as 'SDFs,' additional responsibilities may apply, such as appointing a data protection officer, engaging an independent data auditor, and conducting DPIAs to mitigate risks.

Data retention post-employment

The employer must erase personal data once it is reasonable to conclude that the specified purpose has been fulfilled, unless retention is required to comply with any legal obligations.

Employers in India must adhere to statutory compliance by retaining specific records and employee data for mandated periods, either in original or electronic form, as outlined in various labour laws. For example, the Employees' Provident Funds and Miscellaneous Provisions Act, 1952 does not specify a clear retention period but suggests retaining records for 7 (seven) to 10 (ten) years, while the Employees' State Insurance Act, 1948 mandates 5 (five) years.

Processing of personal data of employees with disabilities

The DPDPA requires data fiduciaries, including employers, to adopt heightened safeguards when processing the personal data of employees who are persons with disabilities. The data fiduciary's responsibilities are amplified in these cases, as information related to disabilities may inherently include sensitive personal data. Such data, if disclosed or misused, has the potential to lead to discrimination or other adverse effects for the employee. Employers are therefore advised to establish specific protocols that ensure compliance with the DPDPA's mandates on data protection while also upholding principles of equality and non-discrimination.

Processing of employee data for background verification

The DPDPA does not definitively state whether 'purposes of employment' includes data collection for recruitment, such as pre-employment background checks, where an employer-employee relationship isn't yet formalised. However,

the DPDPA's broad framework could reasonably support background verification as an essential step in employment, allowing employers to filter suitable candidates and manage future workforce needs. To ensure compliance, employers should clearly document the purpose of this data processing, provide necessary notifications to candidates, and follow the DPDPA requirements, minimising compliance risks. Employers frequently rely on third-party providers for high-risk data processing tasks, such as background checks, behaviour analytics, health insurance, and financial benefits. Under the DPDPA, employers should implement a thorough due diligence process and ensure that third parties processing employee data operate under formal data processor agreements with stringent security and privacy safeguards.

Managing international employee data

The DPDPA introduces specific cross-border data transfer exemptions that can reduce compliance burdens for certain fiduciaries, including employers, when handling data of non-Indian employees. These exemptions allow eligible employers more flexibility in transferring data across borders, though they must still adhere to core accountability and data security obligations under the DPDPA. Employers invoking these cross-border exemptions need to balance operational needs with ongoing compliance, as the exemptions are context-specific and require clear substantiation of eligibility. Additionally, the DPDPA grants the Central Government authority to restrict transfer of data of Indian residents to designated countries via notifications, meaning that employers must stay vigilant to ensure alignment with both the DPDPA standards and any stricter requirements imposed by other applicable laws.

> Under the DPDPA, the Central Government has the authority to impose restrictions on data transfers to certain countries, which will be specified through notifications. It is crucial to note that if any other applicable law imposes stricter restrictions on an employer regarding such transfers, those restrictions will take precedence.

Startups under the DPDPA

The DPDPA has introduced a distinct category for startups, recognising the unique position they occupy within the economy and the challenges they may face in terms of compliance. A 'startup', as per the DPDPA, is a private limited company, partnership firm, or limited liability partnership that has been incorporated within India and meets specific criteria established by the Central Government's relevant department. By categorising eligible entities as startups, the DPDPA allows certain relaxations in data processing obligations, offering a more proportionate regulatory approach. For employers in this category, these relaxations aim to mitigate compliance burdens during the early stages of business growth. Nonetheless, it remains incumbent upon startups to prioritise compliance with accountability and security safeguards, as these obligations form the core of responsible data fiduciary practices under the DPDPA.

Processing of employee data to safeguard employer's interests

The processing of personal data to safeguard the employer from loss or liability is allowed under the DPDPA. The DPDPA provides a wide definition for 'loss', therefore instances such as processing of personal data for prevention of financial fraud or corporate espionage, or misuse of resources, prevention of reputational damage, or processing personal data for enforcement of legal claims, could be some of the examples for processing for safeguarding from loss or liability.

The processing of personal data to protect the employer's trade secrets, intellectual property and classified information is allowed under the DPDPA. Some of the instances for maintenance of confidentiality could include implementing access control mechanisms, to enter into non-disclosure agreements with the employees, tracking of company's information technology assets with the employees, etc.

Privacy and data protection in Artificial Intelligence

In the era of Artificial Intelligence ("**AI**"), the use of big data including personal data is considered to be indispensable in the training, development and deployment of AI systems. Personal data is leveraged at various stages, such as during the training of AI models, where vast datasets are processed to enable the AI model or system to identify patterns, and during the working of the AI system, where personal data may be continuously collected, analysed, and processed for the AI system to generate outputs. However, this extensive use of personal data raises significant privacy concerns, particularly regarding data protection, transparency, and accountability.

Applicability of the DPDPA

An entity processing personal data for training, development or deployment of the AI models or system in India → needs to comply with the provisions of the DPDPA ← An entity outside India processing personal data for training, development or deployment of AI systems in connection with offering goods or services to data principals in India

In cases where entities outside India profile data principals located in India only for the purpose of training AI models, and the resulting systems are subsequently not made available in India, there could be enforcement issues as the DPDPA does not apply to processing of personal data outside India that is not in connection with offering goods or services to data principals in India.

Training on publicly available data

The DPDPA does not apply to the processing of personal data that has been made publicly available by the data principal themselves, or by any person who is legally mandated to make such data publicly available

The DPDPA exempts publicly available data from its scope, allowing unrestricted use for training Machine Learning/AI models, including through data scraping. Unlike Singapore's PDPA, which maintains some safeguards, the DPDPA imposes no obligations if the data is made public by the data principal or through legal mandates. This contrasts sharply also with the EU's GDPR, which applies to all personal data, including public data. The European Data Protection Board's ChatGPT Taskforce has warned that scraping publicly available data, especially sensitive data, risks individual rights and requires safeguards to prevent misuse. The Belgian Data Protection Authority aligns with this perspective by requiring proportionality and data minimisation when personal data is processed.

In the United Kingdom, the Information Commissioner's Office highlights the need to adhere to GDPR principles even when processing publicly available data, stressing that such data is not exempt from privacy laws. This includes complying with lawful bases for processing, transparency, and ensuring data subjects' rights are protected

The ability to process publicly available personal data without any legislative oversight will give rise to 'invisible processing' where the data principals are not aware of the purpose for which their personal data is processed.

Where the AI model is trained on anonymised data, the DPDPA is not applicable as it does not qualify as 'personal data'.

Scraping publicly available data may not be covered under the DPDPA but could still result in other violations like breach of intellectual property rights, breach of contract, or unauthorised access under other applicable laws.

Legitimate uses for processing

Under the DPDPA, 'legitimate use' serves as a lawful basis for processing personal data without explicit consent, provided the processing aligns with certain specific, predefined purposes in the DPDPA. Legitimate use comprises processing for functions such as State operations, health emergencies, medical purposes, employment, and other uses listed under Section 7 of the DPDPA. The application of legitimate use, however, requires compliance with the principle of purpose limitation. It is common practice to repurpose personal data obtained for a primary purpose to train AI models. However, post the implementation of the DPDPA, the data fiduciaries will have to reassess the grounds for processing to either obtain specific consent to process personal data or rely on the legitimate use for training or working of AI models. Where AI is used to automate decision-making or make inferences about an individual, such processing may also generate new personal data. The data fiduciaries should ensure that they rely on a ground for the processing of this newly generated personal data as well.

AI in law enforcement and State functions

1. DPDPA allows the State or its instrumentalities to process personal data to provide or issue various benefits, services, or permits to data principals based, as a legitimate use. This enables the State and its instrumentalities to process citizen data to develop or deploy AI to augment administrative capacity. For example, states like Tamil Nadu, Telangana, and Andhra Pradesh are leveraging AI to improve public service delivery - such as water body management, pensioner authentication, and real-time beneficiary identification. These applications demonstrate how AI can not only streamline administrative functions but also create a more inclusive and responsive system of governance, reflecting a broader trend in AI-driven public services. The DPDPA does not create a bar on such use cases.
2. It is also, not uncommon for AI tools, particularly Automated Facial Recognition Technology (AFRT), to be integrated into law enforcement for tasks such as identifying criminals or locating missing persons. In some instances, AI is also used in predictive policing, helping authorities allocate resources effectively by predicting where crimes may occur. Similarly, AI applications are being tested for disaster management, ensuring the safety of citizens during calamities. However, such tools can facilitate constant monitoring of individuals in public spaces, posing risks to privacy rights, especially since, the processing of personal data in the interest of prevention, detection, investigation or prosecution of crimes or any contravention of any law in India is exempted from certain provisions of Chapter II of the DPDPA. Without proper policy or regulation, such surveillance can lead to an adverse effect on free expression and create an environment of pervasive monitoring.
3. Another significant concern is the potential for bias in AI systems. If AI models are trained on biased historical crime data, they may unintentionally reinforce existing prejudices. This can lead to discriminatory outcomes, such as unfairly targeting specific communities or perpetuating stereotypes. Furthermore, the lack of transparency in how AI algorithms process data can make it challenging to identify and address such biases, amplifying the risk of systemic inequities.

Processing of personal data belonging to children/persons with disabilities

If the training dataset contains personal data belonging to either children or persons with disabilities, or if an AI system processes such personal data, the data fiduciary must obtain verifiable consent of the parent or legal guardian (as may be applicable), in the manner as may be prescribed by the rules to the DPDPA.

1. Although the DPDPA prohibits the processing of personal data to undertake behavioural monitoring of children or advertisements targeting children, such a similar prohibition is not present for processing of adults' personal data. The DPDPA should recognise the principles of *Responsible AI* and allow adult data principals to either object or restrict the processing of personal data for automated decision making, profiling or targeted advertising. This right is provided under the GDPR, where the processing is undertaken by relying on the legitimate interest or if the processing is necessary for the performance of a task carried out in the public interest.
2. The Central Government can notify classes of data fiduciaries who may not be required to obtain verifiable consent or who can undertake behavioural monitoring or target advertising on children.

Research and innovation

The DPDPA provides specific exemptions to support innovation and research while balancing privacy rights. These include:

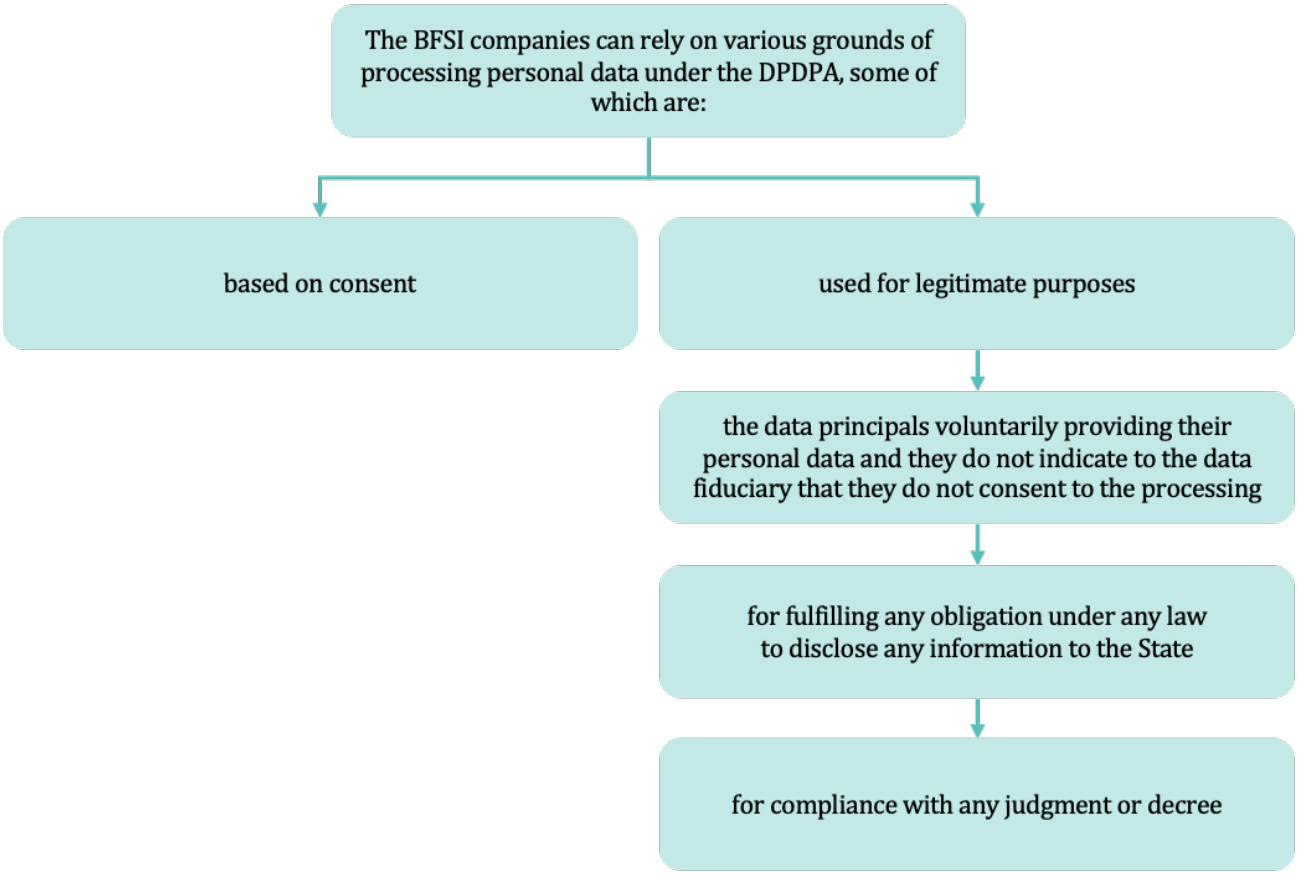
1. **Startup exemptions**: Startups notified by the Central Government are exempt from certain provisions to foster innovation and reduce compliance burdens during their growth phase, including in areas like AI and emerging technologies.
2. **Research**: Personal data may be processed for research, archiving, or statistical purposes if it is not used to make decisions specific to a data principal, and such processing is carried out in accordance with the prescribed standards to be set by the rules to the DPDPA.

Impact of data protection laws on the Banking, Financial Services and Insurance sector

The application of DPDPA to the Banking, Financial Services, and Insurance ("**BFSI**") sector poses unique challenges and opportunities to the existing, well-defined regulatory landscape. With robust frameworks already prescribed by the RBI, the Insurance Regulatory and Development Authority of India ("**IRDAI**"), and the Securities and Exchange Board of India ("**SEBI**"), the BFSI sector already adheres to stringent data protection norms. However, the DPDPA introduces broader principles that address gaps, particularly in areas such as individual rights and consent specificity.

Grounds for processing personal data

Under the DPDPA there are 2 (two) valid grounds for processing: consent; and for legitimate purposes. The BFSI sector has long operated on the principle of informed consent, as emphasised by RBI, SEBI, and IRDAI guidelines. For example, the RBI's KYC Directions ensure that individuals provide explicit consent for data collection during onboarding processes. However, these consent mechanisms often encompass broad purposes, such as transaction facilitation or compliance, without specification. The DPDPA refines the concept of consent, emphasising explicit, specific, and purpose-bound agreements. This adds a layer of granularity that BFSI entities must integrate into their consent frameworks. This requires operational shifts, such as updating consent forms and refining digital interfaces to ensure clarity and compliance.



The concept of a consent manager under the DPDPA could be similar to the RBI's AA framework, introduced under the Master Directions - Non-Banking Financial Company - AAs (Reserve Bank) Directions, 2016. This framework envisioned intermediaries facilitating secure, user-controlled sharing of financial data. These AAs act as consent managers, ensuring that individuals retain control over their data while enabling seamless data sharing between financial institutions. Under the DPDPA, the consent manager concept is expanded to apply across sectors, providing tools for users to manage and revoke consent efficiently.

The existing BFSI regulations allow data processing under legal mandates, such as anti-money laundering requirements or fraud detection. This is broadly in line with processing personal data, without consent, for legitimate uses such as compliance with laws of India or to comply with a judgement, decree or order issued under Indian laws, as given under the DPDPA. Entities operating in the BFSI sector may sometimes need to disclose or share data for compliance with foreign regulations or orders or to work with other companies that are required to meet their foreign obligations. In such cases the entities would need to carefully consider the grounds for such data processing.

Role in processing personal data

Under the DPDPA, the BFSI entities and other entities in the financial ecosystem cannot operate under a fixed assumption that they will always fall under a single role, be it data fiduciary or processor. Their role under the DPDPA would depend on the specific context of data processing in each use case. This fluidity of roles necessitates a case-by-case evaluation, considering factors such as the origin of data, contractual obligations and the control exercised over the data's use. Therefore, all organisations in the financial ecosystem must meticulously analyse their data flows and processing arrangements to correctly identify their role which would in turn influence the kind of obligations they would have under the DPDPA.

Enhanced obligations for BFSI entities

Under the DPDPA, it is highly likely that BFSI entities could be classified as SDFs given that their core operations involve processing sensitive data and the potential risks to individual's privacy in the event of a breach. These entities may collect and process data like financial details, aadhaar, permanent account number and biometric information for purposes such as 'know your customer' compliance, credit approvals and fraud prevention. If designated as SDFs, BFSI entities will be required to comply with enhanced obligations, including conducting DPIAs, appointing a DPO and undergoing independent data audits.

Existing regulations, such as RBI's guidelines on cybersecurity, SEBI's data handling norms for intermediaries and IRDAI's privacy-related directives, further reinforce the specific responsibilities of BFSI organisations. The sector's reliance on digital platforms, AI tools and data-driven decision-making makes compliance with the fiduciary obligations under the DPDPA a natural extension of their regulatory obligations. These entities are well-positioned to meet the core requirements for lawful, fair and transparent data processing mandated by the DPDPA.

For entities in the BFSI sector, this would mean aligning their compliance efforts under the DPDPA with existing regulatory frameworks while investing in robust data governance mechanisms. Proactively preparing for this designation will not only ensure compliance but also build greater trust with customers and stakeholders in an increasingly data-driven financial environment.

Cross-border transactions and DPDPA

The Central Government, by notification may restrict transfer of personal data outside India to certain countries or territories. The DPDPA mentions that sectoral legislations will supersede the provisions of the DPDPA where there is transfer of personal data outside India. In the BFSI sector there are various sectoral laws that mandate data localisation and regulate the transfer of personal data outside India. These sectoral requirements add layers of complexity to cross-border data processing and necessitate BFSI entities to implement robust data governance frameworks.

For instance, the RBI mandates that payment system data be stored in India, impacting payment intermediaries and financial institutions handling transaction data. Similarly, insurance companies must adhere to the regulations of the IRDAI, which imposes specific restrictions on cross-border data flows.

To comply with both the DPDPA and sectoral mandates, the BFSI institutions must assess their data processing activities, ensure localisation requirements are met and establish agreements with service providers detailing compliance with cross-border data transfer rules. Furthermore, leveraging privacy-enhancing technologies such as encryption and anonymisation can mitigate risks associated with permitted international data transfers while adhering to regulatory expectations.

Consistency between DPDPA and sectoral regulations

While RBI, IRDAI and SEBI frameworks emphasise data security and governance, they lack comprehensive mechanisms for addressing individual rights. The DPDPA introduces rights for individuals, including the right to access, correction and erasure, which BFSI entities must now accommodate. Requests for data erasure may specifically pose challenges due to retention obligations mandated under different applicable laws.

While sectoral regulations mandate privacy disclosures, the DPDPA requires detailed privacy notices that explicitly outline data processing purposes, storage durations and cross-border transfer mechanisms. This demands a review of privacy policies, ensuring they are comprehensive yet easily comprehensible.

The DPDPA complements the BFSI sector's existing frameworks, addressing gaps in individual-centric rights and introducing a harmonised approach to global data governance. However, it also presents challenges in reconciling the variance in the sectoral guidelines and DPDPA.

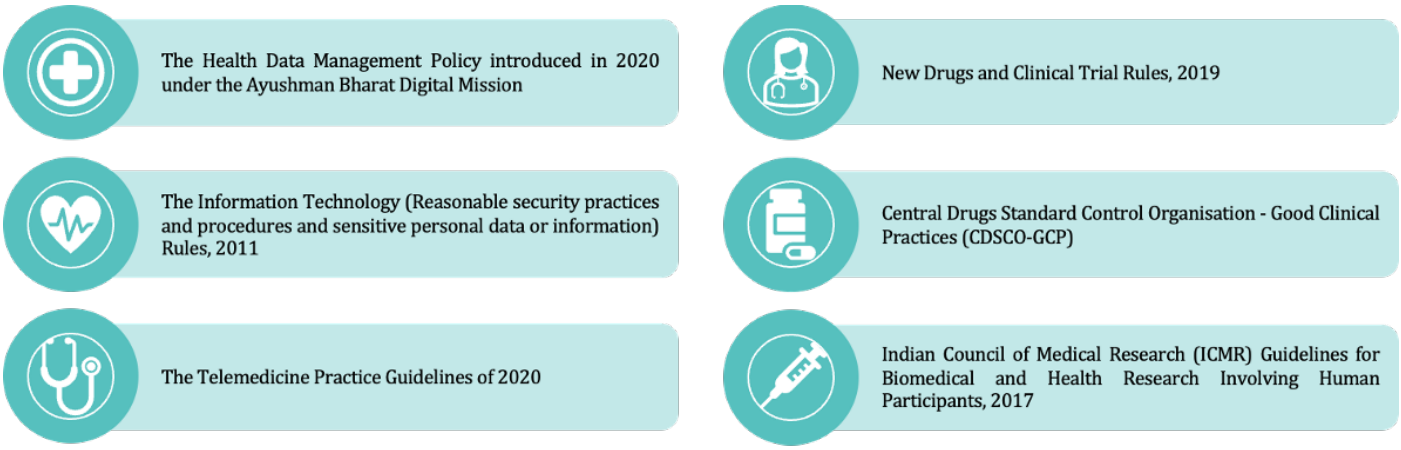
Navigating privacy requirements for healthcare and pharmaceutical sectors

The healthcare and pharmaceutical sectors in India are at a critical juncture concerning data protection and privacy. Despite the growing reliance on digital health records and technology, the regulatory framework remains fragmented to address the complexities of modern healthcare data ecosystems. The DPDPA introduces a new paradigm for data protection, but its integration with the healthcare and pharmaceutical sector's unique requirements presents challenges and opportunities.

The current regulatory landscape governing health data in India

India currently lacks a comprehensive law addressing healthcare or patient data, unlike the United States' Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**"). Enacted to safeguard patient privacy, regulate the use and disclosure of protected health information, and promote efficiency and interoperability in healthcare, HIPAA serves as a robust framework for managing health information in the USA. In India, an attempt to introduce similar protections through the Digital Information Security in Healthcare Act, 2018 focused on regulating digital health data with strict security, consent, and accountability measures has failed to progress. Instead, the healthcare sector remains governed by a patchwork of sectoral regulations. Instead, there is a patchwork of regulations that apply to processing health and patient data.

Overview of key sectoral regulations applicable to this sector currently



1. **The Health Data Management Policy ("HDM Policy")**: The HDM Policy v.2, released in 2022, by the Ministry of Health and Family Welfare, sets the minimum standards for privacy and data protection within the Ayushman Bharat Digital Mission ecosystem. The HDM Policy mandates that no health data be shared with entities, including insurance and pharmaceutical companies, without the individual's consent. It imposes purpose-based limitations on data sharing and requires health information users to refrain from further disclosing data without the data principal's consent. Additionally, shared data must not be stored beyond the period necessary for the specified purpose, and the principle of data minimisation must be adhered to by entities receiving the data.
2. **The SPDI Rules**: The SPDI Rules, issued under Section 43A of the Information Technology Act, 2000, establish a framework for handling sensitive personal data, including health information. The SPDI Rules define Sensitive Personal Data or Information ("**SPDI**") to include medical records, biometric information, and physical or mental health conditions. Organisations collecting SPDI are required to publish a privacy policy, clearly disclose their data

collection and processing practices, and secure informed consent from individuals before collecting or sharing their data. The rules emphasise implementing stringent security measures, such as encryption and access controls, and require organisations to appoint a grievance officer to address complaints. Non-compliance can attract civil liability for negligence, underscoring the SPDI Rules' role in ensuring accountability and data protection, particularly in sectors like healthcare that handle highly sensitive information. When the DPDPA comes into force, the SPDI Rules will automatically be repealed.

3. **The Telemedicine Practice Guidelines of 2020**: The Telemedicine Guidelines emphasise that Registered Medical Practitioners ("**RMPs**") must adhere to the Indian Medical Council Act ("**IMC Act**") and professional ethics regarding patient privacy and confidentiality. RMPs must also comply with relevant data protection laws, including the Information Technology Act, 2000 and take reasonable care when selecting services to prevent breaches of patient confidentiality. RMPs will not be held responsible for confidentiality breaches due to technology or third-party failures if proper care is exercised. Misconduct, including forcing teleconsultations when in-person is requested, misusing patient data, and violating privacy laws, is strictly prohibited. Penalties for violations are in line with the IMC Act and other applicable laws.
4. **The New Drugs and Clinical Trial Rules, 2019 ("CTR")**: CTR forms the core regulatory framework for conducting clinical trials in India. These rules govern the approval process, ethical considerations, and conduct of clinical trials. Key provisions include the need for ethics committee approval before initiating a trial and the submission of trial protocols to the Central Drugs Standard Control Organisation ("**CDSCO**") for review. CTR also mandate compliance with international standards to ensure the integrity of data and the safety of trial participants. A critical requirement under the CTR is the obligation to obtain informed consent from participants, ensuring they are fully informed about the risks, benefits, and purpose of the trial before their participation.
5. **CDSCO – Good Clinical Practices Guidelines ("CDSCO - GCP Guidelines")**: The CDSCO – GCP Guidelines outline the ethical and scientific quality standards for clinical trials. These CDSCO – GCP Guidelines are in line with international best practices and focus on protecting the rights and safety of participants while ensuring the reliability of trial data. The CDSCO – GCP guidelines emphasise the need for strict adherence to safety protocols, confidentiality, and transparency in reporting trial results. They also reinforce the requirement for informed consent to ensure participants understand the potential risks and benefits associated with their involvement in clinical trials.
6. **Indian Council of Medical Research Guidelines for Biomedical and Health Research Involving Human Participants, 2017("ICMR Guidelines")**: ICMR Guidelines provides additional ethical guidance for biomedical research in India. The ICMR Guidelines focus on the protection of human participants and emphasise the need for informed consent before any research is conducted. They ensure that participants are not coerced or misled and that their rights are upheld throughout the research process. The ICMR Guidelines also establish standards for research ethics committees, data management, and the dissemination of results, all while ensuring compliance with national and international ethical standards in health research.

With the DPDPA now in place, healthcare and pharmaceutical entities must navigate these fragmented regulations and the broader obligations under the DPDPA.

Transformative implications of the DPDPA on the healthcare and pharmaceutical sectors

The DPDPA introduces comprehensive provisions to strengthen data protection across sectors, including healthcare. The DPDPA mandates a higher degree of accountability for SDFs which may include entities processing large volumes of sensitive data such as health data. Health data, while not explicitly classified as sensitive personal data under the DPDPA, may be treated with the same level of protection due to the context provided by the SPDI Rules. This ensures stricter regulations on its processing, storage, and sharing.

The following points outline the key provisions of the DPDPA that influence the regulation of health and patient data in India.

Consent

A central feature of the DPDPA is its requirement of specific, informed, affirmative consent, which places the patient at the core of its protections. The DPDPA requires explicit, informed consent from individuals for the collection and processing of their health data. This empowers patients to make well-informed decisions about how their data is used and shared. The DPDPA also provides individuals with the right to withdraw their consent at any time, further reinforcing their control over personal information. For healthcare entities, this means establishing patient-centric mechanisms for obtaining and managing consent, which ensure that data collection aligns with lawful, specific purposes.

Processing for legitimate uses

The DPDPA provides for the processing of personal data without explicit consent in certain situations.

In the context of healthcare, the DPDPA permits data processing during medical emergencies involving threats to life or health. It also allows processing to provide medical treatment or health services during public health crises, such as epidemics or disease outbreaks. These provisions enable delivering lifesaving care without the requirement of going through a consent mechanism.

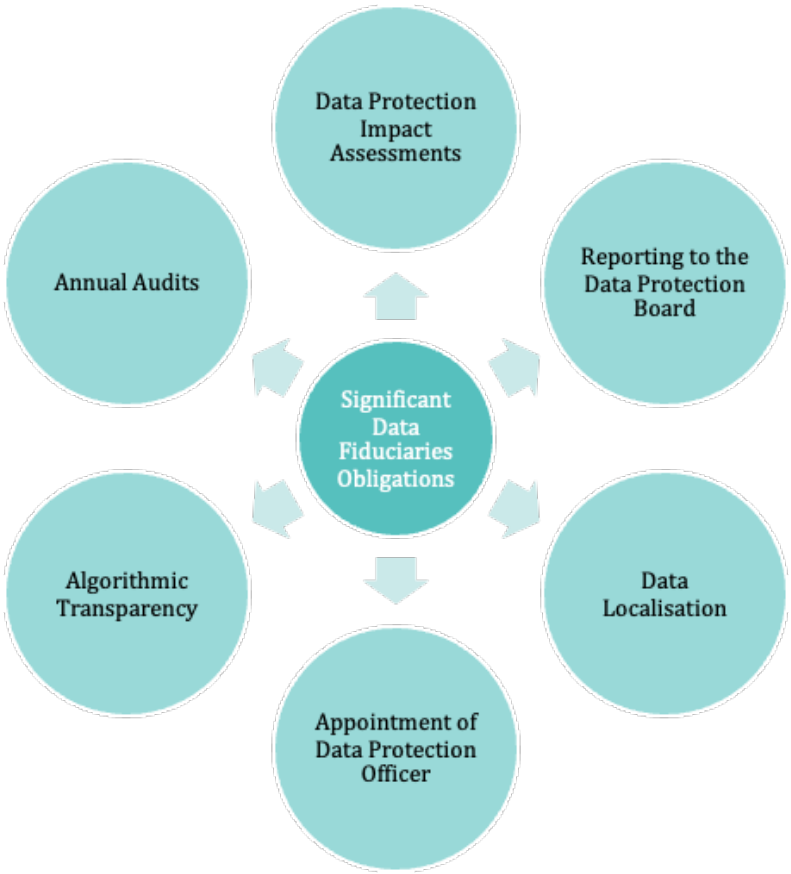
Security obligations for data fiduciaries

The DPDPA requires data fiduciaries to implement measures to protect personal data from breach. The Draft Digital Personal Data Protection Rules, 2025 ("**Draft Rules**") enumerate some security measures including encryption, obfuscation, or virtual tokens to secure personal data, access control mechanisms maintaining logs and monitoring access patterns and reviewing them to detect unauthorised access. In the event of a breach or compromise, data fiduciaries must have measures in place to continue processing data, such as data backups, and ensure that the breach does not hinder the ongoing availability or integrity of the data.

The DPDPA and Draft Rules also make it the data fiduciary's responsibility to ensure that data processors also implement appropriate technical and organisational measures for data protection and comply with the same high standards of data protection.

Enhanced obligations for SDFs

A key feature of the DPDPA is the introduction of a class of SDFs, which is likely to include entities handling such sensitive data like health or patient data. These SDFs have enhanced obligations under the DPDPA and must implement stringent safeguards to protect patient privacy.



SDFs are required to conduct annual DPIAs to identify and mitigate risks associated with their processing operations, particularly in scenarios involving high-risk data usage. Annual audits are also mandatory, with significant findings required to be reported to the Board, thereby enhancing regulatory oversight. To promote fairness, SDFs are obligated to ensure algorithmic transparency, which includes measures to detect and prevent biases in automated decision-making processes. Data localisation measures may also apply, requiring critical or SPDI to be stored within India to strengthen data security and uphold sovereignty. Furthermore, SDFs must establish efficient grievance redressal mechanisms to address data principals' complaints in a timely manner and appoint a Data Protection Officer in India to oversee compliance and act as a liaison with the Board. These obligations reflect the DPDPA's focus on safeguarding personal data, promoting transparency, and ensuring accountability.

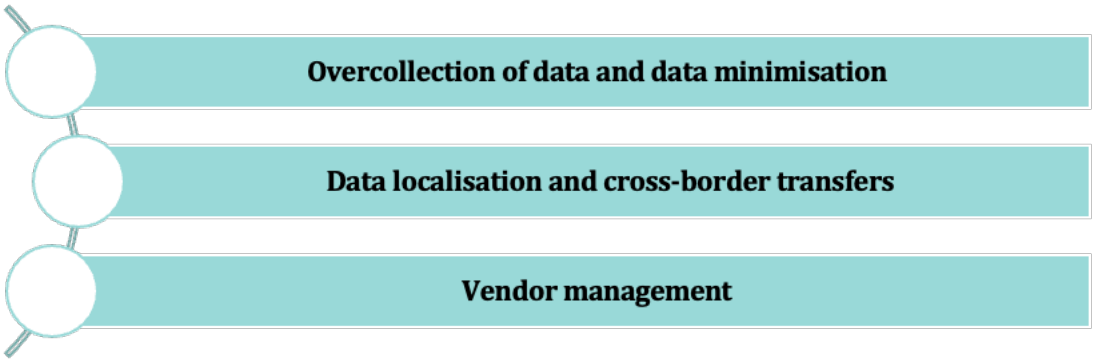
Processing data of children and persons with disability

As a rule, the DPDPA requires data fiduciaries to obtain verifiable consent from a child's parent or lawful guardian before processing the child's personal data. This consent must be acquired with due diligence to verify the identity of the parent or guardian, using reliable identity and age details or government issued ID. For the healthcare and pharma sectors, this means that any collection or processing of children's personal health data will require parental consent protocols that can be verified. Additionally, the DPDPA also prevents tracking and behavioural monitoring of children.

In view of any imminent threats to the health of a child, the Draft Rules do provide for exceptions to the rule of consent and bar on tracking and behavioural monitoring. A data fiduciary who is a clinical establishment, mental health establishment, healthcare professional or an allied healthcare professional like a trained individual supporting diagnosis, treatment, and healthcare plans, does not need parental consent and may undertake behavioural monitoring of children or targeted advertising directed at children to the extent necessary for the protection of her health. What will be considered 'necessary' and 'for the protection of health' will need to be justified by the data fiduciaries. It will thus become important to have internal protocols identifying situations where the rule on consent and behavioural monitoring/tracking can be ignored by the healthcare establishment or health professionals.

Addressing operational challenges in privacy in healthcare

The healthcare sector may face some unique challenges in aligning with the DPDPA's compliance requirements.



Overcollection of data and data minimisation

One of the key concerns in the healthcare sector is the over-collection of data, particularly during patient onboarding or diagnostic processes. Historically, healthcare providers may have collected large volumes of data to ensure comprehensive coverage of potential medical needs. However, under the DPDPA, healthcare providers must reassess their data collection practices to ensure that only the data necessary for the intended medical purpose is collected and processed. Healthcare providers and allied providers will need to establish clear criteria for data collection, map it to certain diagnostic or treatment plans, limit unnecessary data requests, and ensure that any additional data collected is strictly essential for patient care. This shift will require continuous training, updates to internal processes, and close monitoring to ensure that data minimisation is adhered to at every stage of patient interaction.

Data localisation and cross-border transfers

Additionally, healthcare providers may have to navigate the operational complexities of cross-border data transfers. Many providers depend on global systems for storing, analysing, and sharing patient data, leveraging international expertise to enhance healthcare delivery. For SDFs, the Central Government can restrict the transfer of personal data to countries or territories outside India and in some cases even mandate data localisation. It will thus become important for all providers in the healthcare ecosystem to understand where data is flowing and have mechanisms to flow down transfer restrictions, if needed. Localisation mandates also necessitate substantial investment in local infrastructure, reassessment of global partnerships, and the establishment of India-based storage and processing systems. By aligning operations with these localisation requirements, healthcare providers can balance regulatory compliance with operational efficiency in a rapidly evolving data governance landscape.

Vendor Management

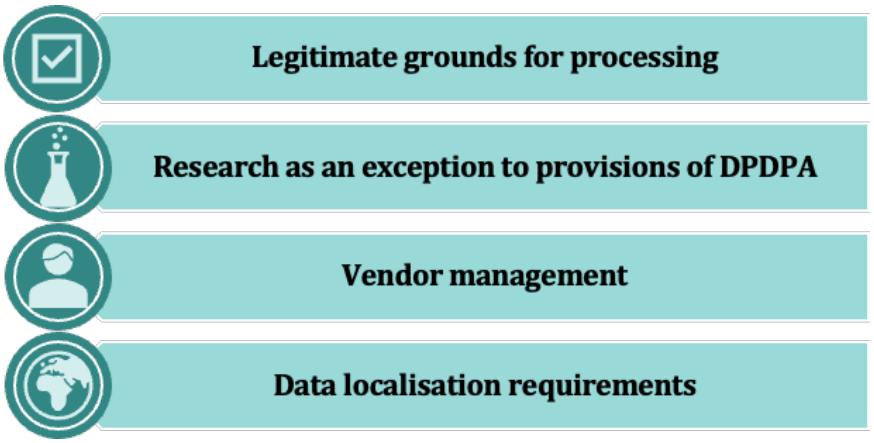
In addition to the challenges of data protection compliance and cross-border data transfers, vendor management is another crucial operational consideration for healthcare providers. Healthcare organisations often collaborate with partners and third-party vendors for a variety of services, such as data storage, software solutions, insurance and analytics. These third parties may have access to sensitive patient data, raising the need for stringent data protection measures in contracts with them.

The DPDPA requires that when a healthcare provider, as a data fiduciary, engages a data processor, they remain responsible for the processor's acts and omissions. Vendors are only allowed to process personal data under the instructions of the data fiduciary in an appropriate contract. The data fiduciary also has the responsibility to ensure that their processors are keeping data safe and following the instructions of the fiduciary for erasure. The Draft Rules also emphasise the need for proper contracts and compliance checks to ensure third-party vendors meet the required

data security standards. This makes it crucial for healthcare providers to implement robust vendor management practices from due diligence to efficient contracts to audits.

Challenges and opportunities in privacy in the pharmaceutical sector

DPDPA presents some challenges for the pharmaceutical sector too, particularly in handling sensitive patient data and data relating to clinical trials. Pharmaceutical companies process large volumes of patient data, including health records and clinical trial data. With the DPDPA, companies must adapt their existing processes and technologies to ensure compliance, especially in patient consent management.



Legitimate grounds for processing

Under the DPDPA, several legitimate grounds for processing personal data without consent are explicitly applicable to delivering healthcare, such as responding to medical emergencies, providing treatment during epidemics or disease outbreaks, and ensuring safety during disasters. These provisions allow healthcare providers to process data directly related to patient care and public health without explicit consent. However, the pharmaceutical sector operates differently, often focusing on clinical trials, drug development, and long-term data collection rather than immediate healthcare delivery. These activities typically do not fall under the same exemptions. For instance, while a pharmaceutical company may process data during a government-mandated vaccination program under the public health exception, ongoing clinical trials or pharmacovigilance activities may still require explicit consent from individuals. The distinction lies in the scope of application i.e., healthcare providers directly deliver care, whereas pharmaceutical companies are often a step removed. This creates a complex compliance landscape for pharma companies, requiring them to carefully evaluate which legal grounds apply to their operations and implement robust consent management systems to address activities that fall outside the scope of healthcare exemptions. Failure to do so risks non-compliance with the DPDPA's stringent requirements.

Research as an exception to provisions of DPDPA

Under the DPDPA, personal data being processed for research, archiving, or statistical purposes, is exempted from the provisions of the DPDPA, provided the processing is carried out in accordance with some standards that the Draft Rules prescribe.

In the pharmaceutical sector, this exemption is crucial for activities such as clinical trials and medical research, where data usage often extends beyond the scope of initial collection. Pharmaceutical companies can process sensitive health data for research purposes, but they must ensure compliance with the standards the Draft Rules lay down, including ensuring data accuracy, notifying data principals of their rights, safeguarding the data through robust security measures, implementing grievance redressal and ensuring that the processing remains proportionate and necessary for the research objectives.

Vendor management

Vendor management is a key operational concern for pharmaceutical companies too. Pharma organisations regularly collaborate with external vendors, distributor or partners for marketing or manufacturing services.

The DPDPA requires that when a healthcare provider, as a data fiduciary, engages a data processor, they remain responsible for the processor's acts and omissions. Vendors are only allowed to process personal data under the instructions of the data fiduciary in an appropriate contract. The data fiduciary also has the responsibility to ensure that their processors are keeping data safe and following the instructions of the fiduciary for erasure. The Draft Rules also emphasise the need for proper contracts and compliance checks to ensure third-party vendors meet the required data security standards. This makes it crucial for healthcare providers to implement robust vendor management practices from due diligence to efficient contracts to audits.

Data localisation requirements

The DPDPA specifies that the Central Government may proscribe personal data transfer to certain countries or regions. The Draft Rules go a step further and lay down that the Central Government may also prescribe certain requirements for transfer of data. Additionally, for SDFs that Central Government may also mandate that all data, including the traffic data be localised only in India.

Localisation mandates necessitate substantial investment in local infrastructure, reassessment of global partnerships, and the establishment of India-based storage and processing systems.

It thus becomes critical for pharma companies to understand and map their data flow, not only across their systems but also those of their partners and vendors.

Privacy issues in deploying AI in the healthcare and pharmaceutical sectors

In the healthcare and pharmaceutical sectors, AI holds great promise for enhancing patient care, improving operational efficiencies, and advancing medical research. AI is being utilised in drug discovery, diagnostics, clinical decision-making, supply chain management, and clinical trials, among other areas. By analysing large datasets, AI accelerates research, aids in the identification of potential drug candidates, and optimises clinical trial designs, ensuring safer and more effective treatments.

However, as AI's role in processing personal health data expands, it raises significant data privacy concerns. A primary issue is the sheer volume of personal health data being processed by AI systems. This not only increases the risk of data breaches but also raises compliance challenges. The DPDPA emphasises data minimisation, a principle that requires that personal data collected be limited to what is necessary for the intended purpose. The growing use of AI in healthcare intensifies the need to ensure that only relevant data is processed and retained, in compliance with this core principle.

AI algorithms, especially those deployed for processing personal health data, must also be scrutinised to ensure they do not pose a risk to data principals' rights. The Draft Rules require SDFs to carry out due diligence and verify that the algorithmic software used for processing personal data—whether for storage, transmission, or sharing—does not create unintended risks, such as discriminatory outcomes or breaches of privacy.

These rules necessitate that companies employ strict oversight to mitigate any harm to individuals and ensure compliance with the DPDPA's provisions on data protection and privacy. This may require carrying out an impact assessment before AI is deployed for any use.

Consumer health-tech

The use of consumer health technologies, such as wearables and mobile health apps, presents different privacy challenges, particularly in terms of data overcollection and the frequent transfer of data across various platforms. These technologies often collect continuous, real-time health information, which, if not properly safeguarded, can be vulnerable to unauthorised access, misuse, or breaches. Furthermore, as the data is typically processed or shared with multiple third-party vendors and platforms, the risk of data leakage, especially in cross-border scenarios, becomes more pronounced.

Under the DPDPA, data fiduciaries hold primary responsibility for ensuring compliance with the DPDPA, even in instances where data processing is carried out by third-party processors. According to the provisions of the DPDPA, a data fiduciary must ensure that any processing undertaken by its processors on its behalf complies with the law. The fiduciary remains accountable for the actions of these processors, irrespective of any agreements made or the failure of the data principal to uphold their duties under the DPDPA. This legal responsibility necessitates thorough oversight and due diligence by data fiduciaries, requiring them to ensure that processors adhere to data protection principles such as data minimisation, purpose limitation, and safeguarding sensitive health data from unauthorised access or misuse.

The path forward for health and pharma data governance

The DPDPA provides a comprehensive framework for data protection and its true effectiveness will depend on its harmonious integration with existing sectoral regulations. While sectoral regulations currently address important aspects of health and patient data management, they lack the detailed requirements outlined in the DPDPA.

Organisations will need to invest time, resources, and expertise to adapt their processes and meet the stringent data protection standards set by the DPDPA. Additionally, the Draft Rules introduce further refinements to these requirements, requiring continuous assessment and adjustment by healthcare and pharmaceutical entities to ensure full compliance.

Navigating compliance under the Digital Personal Data Protection Act, 2023: Key considerations for Global Capability Centres

India stands as a pivotal destination for Global Capability Centres ("**GCCs**"), playing a significant role in supporting multinational corporations across a spectrum of industries such as information technology, finance, healthcare, and telecommunications. The DPDPA and the subsequent Draft Rules mark a transformative moment in India's digital regulatory landscape, underscoring India's vision to establish a robust digital economy while ensuring stringent privacy safeguards.

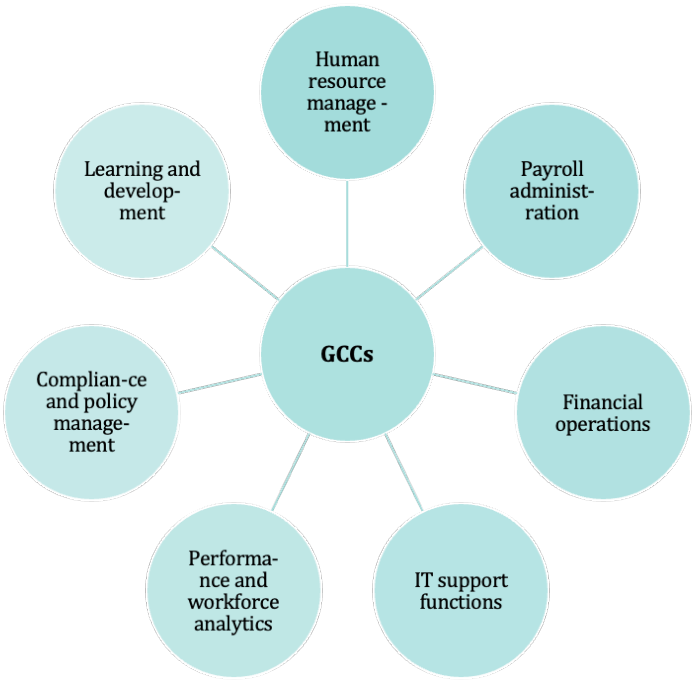
For GCCs, these regulatory developments bring unique challenges and opportunities. GCCs need to comply with the DPDPA while also navigating global laws like the GDPR that may apply to them.

Key Considerations for GCCs *vis-a-vis* the DPDPA

Handling employee data

GCCs handle extensive volumes of employee data as they serve as centralised hubs for managing critical business functions like human resource, payroll, finance, information technology, training, compliance, and workforce analytics on behalf of multinational organisations. Acting as the operational backbone for such functions, they process data to support global operations, enhance efficiency, and ensure compliance with local and international regulations.

Some of their core employment related operations include:



Under the DPDPA, processing personal data typically requires explicit consent from the data principal. However, the DPDPA recognises certain 'legitimate uses' that exempt organisations from obtaining consent, particularly in the context of employment.

These legitimate purposes include core employment-related activities such as:

'the purposes of employment'	or 'those related to safeguarding the employer from loss or liability such as corporate espionage',	'for maintenance of confidentiality of trade secrets, intellectual property, classified information'	or 'for provision of any service or benefit sought by a data principal who is an employee'

However, if the processing of employee data goes beyond these legitimate uses – for purposes unrelated to core employment functions - explicit consent must be obtained from the employee. It thus becomes important for GCC to document what data is collected, the specific purposes for its use and the legal basis for its processing. This may be essential to demonstrate compliance with the DPDPA and to mitigate the risks associated with any unauthorised or non-compliant data processing.

Cross-border data transfers and data localisation

Restrictions on cross-border transfer	Data localisation mandates for significant data fiduciaries	Exemptions for specific transfers

The DPDPA acknowledges the significance of cross-border data transfers, including for GCCs, while prioritising the protection of personal data. Under the DPDPA, the Central Government is empowered to restrict the transfer of

personal data by data fiduciaries to specified countries or territories through notifications. Importantly, the legislation also establishes that its provisions do not override existing sectoral regulations that may impose stricter requirements on data transfers.

The Draft Rules add that the Central Government may prescribe certain requirements even for transfers to approved countries. GCCs must carefully evaluate where employee data is stored and accessed to ensure compliance with these rules.

For GCCs that may be classified as SDFs due to the volume or sensitivity of the data they process, the Draft Rules introduces additional obligations. The Draft Rules prescribe that the Central Government may mandate localisation of certain data, along with related traffic data in India. This makes it crucial for GCCs to be more careful if they are classified as SDFs

There are certain exemptions under the DPDPA that may potentially allow GCCs to be exempt from restrictions on cross-border data transfers. For instance, processing personal data may be exempt if it is necessary for enforcing legal rights or claims, or if it involves the processing of personal data related to a contract entered into with a person outside India. These exemptions could be particularly useful for GCCs, where data is frequently transferred across borders for operational purposes. However, GCCs must carefully evaluate each case to ensure they meet the specific conditions of these exemptions and mitigate any potential compliance risks.

Intra-group transfers

GCCs often perform intra-group transfers to centralise and streamline operations, ensuring efficient use of resources and expertise. Such intra-group transfers of data by GCCs must be conducted in compliance with the provisions laid out for data processing under the DPDPA.

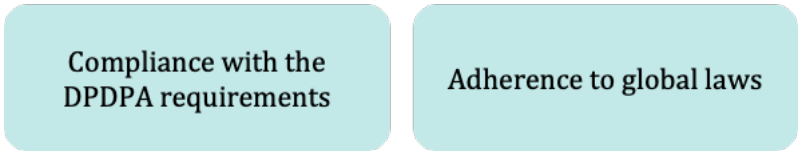
When it comes to group transfers of data, key issues that may arise include maintaining clarity on the legal basis for processing, considering purposes for which personal data may be shared within the group and ensuring that data is transferred outside India in compliance with the DPDPA.

If GCCs already have group policies that align with global laws like the GDPR, these may need to be adapted to meet the DPDPA's requirements, especially where the DPDPA affords more protection or adds restrictions for personal data. To ensure compliance, GCCs may need to review and enhance their internal group transfer policies.

Intersection of global laws and the DPDPA

The intersection of global privacy laws and the DPDPA presents a complex challenge for GCCs, which act as hubs for multinational organisations. As these centres of operations often handle data across various jurisdictions, GCCs are not only required to comply with the data protection regulations of the country they operate in, but also with international laws like the GDPR, United States' Health Insurance Portability and Accountability Act of 1996, California Consumer Privacy Act etc. For example, when processing data of employees in the EU, the GDPR will apply in addition to the DPDPA. Navigating this intersection may require a strategic approach to harmonise policies across diverse legal frameworks while maintaining consistency and compliance. GCCs must carefully consider how global regulations intersect with the DPDPA, particularly in areas such as consent frameworks, data subject rights, data localisation requirements, accountability and cross-border data transfer mechanisms.

Creating globally aligned data policies that incorporate the DPDPA's incremental obligations requires a dual approach:



GCCs may need to develop scalable data governance frameworks that include robust mechanisms for tracking legislative changes in India and abroad. Furthermore, these policies may need to incorporate dynamic compliance monitoring tools and employee training programs tailored to the DPDPA's evolving regulatory landscape.

Third-party/vendor management

GCCs often provide shared services across their global operations, which may involve transferring data received from different countries to downstream vendors, both within India and abroad. As a result, it becomes crucial for GCCs to conduct thorough due diligence on their vendors, ensuring they not only comply with the DPDPA but also adhere to the requirements of relevant global privacy laws. This may include a unified due diligence approach, signing contracts with global protections, an integrated breach management policy and an audit strategy that's globally aligned.

By ensuring that vendor relationships meet both DPDPA and global standards, GCCs can mitigate potential regulatory risks and maintain the integrity of their operations across borders.

The path forward for GCCs

GCCs operate in a complex environment shaped by diverse regulatory requirements and evolving data protection laws. From managing employee data and ensuring lawful cross-border transfers to maintaining oversight over third-party vendors, the challenges are multifaceted and demand careful attention. The DPDPA, Draft Rules, and global laws like GDPR add layers of accountability, requiring GCCs to align their practices with stringent global compliance standards. Navigating these intricate requirements is not just a regulatory necessity but a critical aspect of sustaining seamless operations. As GCCs continue to expand their roles, addressing these considerations will remain pivotal.

Key highlights of the Draft Rules

The draft rules under DPDPA were published by the MeitY, on January 3, 2025. The draft rules provide the details of the implementation and procedural framework of DPDPA.

Key Highlights

	Providing clear and comprehensive notices to the data principals by data fiduciaries
	Conditions for registration of consent managers with the Board and compliance with its obligations
	Processing by the State and its instrumentalities to be done following specified standards
	Reasonable security safeguards to be adopted by the data fiduciary to protect personal data in its possession or under its control
	Data fiduciaries shall intimate data principals and the Board of any personal data breach, promptly
	Period for retention of personal data defined for different classes of data fiduciaries
	Verifiable consent requirements to be followed while processing personal data of children/persons with disabilities
	Additional obligations of a significant data fiduciary including annual audits, reporting to board and data localisation
	Data fiduciaries to have a policy defining the timeline and manner of response to exercise of rights
	Transfer of personal data outside India, may be subject to further Central Government restrictions
	Appointment of members and procedure for meetings of the Board
	Central government may call for information from data fiduciary or intemediary for purposes specified

Notice to the Data Principals:

The draft rules mandate that Data Fiduciaries provide a clear and standalone notice to Data Principals before processing their Personal Data. This notice must ensure that the Data Principal is fully informed and able to make an independent decision regarding their consent. Specifically, the notice must:

Be Independent:

It should not rely on or be combined with any other information provided to the Data Principal, ensuring clarity and focus.

1. **Use Clear and Simple Language:** The notice must present all necessary details in an understandable manner. This includes:
   a) An itemised description of the categories of Personal Data being collected.
   b) The specific purpose for which the Personal Data is being processed.
   c) A description **of the goods or services** enabled through such processing.
2. **Include Accessible Mechanisms:** The notice must provide a communication link, such as a website or app, or other means through which the Data Principal can:

   Withdraw consent with ease comparable to the process of giving consent.
   a) Exercise their rights under DPDPA.
   b) File a complaint with the Board regarding grievances.

Registration and Obligations of Consent Manager:

According to the draft rules, a person wishing to act as a Consent Manager must apply to the Board for registration, provided they meet the conditions specified in Part A of the First Schedule, some of which include incorporation in India, technical and organizational capacity and a net worth of not less than two crore rupees. Once registered, the Consent Manager is subject to the obligations outlined in Part B of the First Schedule, including enabling Data Principals to manage their consent through an interoperable platform and maintaining a record of consents given, denied, or withdrawn by the Data Principal. Additionally, the Consent Manager must ensure that personal data is made available or shared in a manner that prevents its contents from being readable by the Consent Manager itself. The Consent Manager is also required to maintain records of notices accompanying requests for consent and the sharing of personal data with transferee Data Fiduciaries. If the Board determines that the Consent Manager is not adhering to the conditions, it may notify the Consent Manager and direct corrective actions after providing an opportunity for the Consent Manager to be heard. Furthermore, in cases where the Board deems it necessary to protect the interests of Data Principals, it may suspend or cancel the Consent Manager's registration, issue orders, and give directions after offering an opportunity for the Consent Manager to be heard. Additionally, there needs to be periodical reporting to the Board of technical and organizational controls, systems, procedures, and safeguards implemented by the Consent Manager; continued compliance with registration conditions; adherence to obligations under DPDPA and rules; and the outcomes of internal audits conducted to evaluate these aspects.

Processing by the State and its instrumentalities:

DPDPA t allowed the State or its departments to process an individual’s data, without their consent, if it is for providing them any benefit, subsidy, certificate, service, license or permit. The Rules now prescribe standards for processing for such purposes, which include the State adhering to principles of data minimization, accuracy, purpose limitation, reasonable security safeguards, notice and accountability. The rule further clarifies the types of subsidies, benefits, services, certificates, licences, or permits covered under this provision:

Under Law:

Refers to the provision or issuance of these items based on the powers or functions exercised by the State or its instrumentalities under any applicable law.

1. **Under Policy:** Refers to actions taken in accordance with policies or instructions issued by the Central or State Governments, exercising their executive powers.
2. **Using Public Funds:** Refers to the issuance of these items financed by public funds, including money from the Consolidated Fund of India or the respective State, or the funds of local authorities under the control of the Government.

Reasonable security safeguards:

The draft rules impose an obligation on Data Fiduciaries to protect personal data under their control or possession, including data processed by Data Processors on their behalf. Data Fiduciaries must implement reasonable security safeguards to prevent personal data breaches. These safeguards should include, at a minimum, appropriate data security measures, such as encryption, obfuscation, or masking of personal data, or the use of virtual tokens. There must also be measures to control access to computer resources used for processing the data, alongside monitoring and logging systems to detect unauthorized access. Furthermore, Data Fiduciaries must ensure that the availability, confidentiality, and integrity of personal data are maintained in the event of breaches, with provisions for data backups to support continued processing. Logs and data must be retained for up to one year to support investigations and prevent recurrence of unauthorized access. Additionally, Data Fiduciaries are required to include clauses in contracts with Data Processors to ensure that they also implement reasonable security safeguards. This approach establishes a comprehensive framework for safeguarding personal data, ensuring that breaches are swiftly detected, mitigated, and prevented in the future.

Intimation of personal data breach:

The draft rules require Data Fiduciaries to notify Data Principals promptly upon becoming aware of a personal data breach. The notification must be concise, clear, and provided without delay, through the Data Principal's user account or another registered communication channel. The breach notification must include a description of the breach, detailing its nature, extent, timing, and location. It should also inform the Data Principal of the potential consequences, any measures taken or being taken by the Data Fiduciary to mitigate risks, safety steps the Data Principal can take to protect their interests and contact details of a representative who can address queries related to the breach.

Data Fiduciaries must notify the Board about the breach in two stages. First, they must promptly inform the Board of the breach's nature, extent, timing, and likely impact. Second, within 72 hours or an extended period as approved by the Board, they must provide more detailed information, including the circumstances leading to the breach, measures to mitigate risk, findings about the responsible party, steps to prevent recurrence, and a report on the notifications sent to affected Data Principals.

Data Retention Period:

The draft rules specify that the period for erasure of personal data, as outlined in Schedule III, varies depending on the class of Data Fiduciary, such as e-commerce entities, online gaming intermediaries, and social media platforms. These entities may retain personal data for up to three years from the last interaction with the Data Principal or from the commencement of the rules, whichever is later. However, this retention period may be extended if retention is required by law.

Before erasure, Data Fiduciaries must notify the Data Principal at least 48 hours in advance. This notification should inform the Data Principal that their data will be erased unless they log into their user account or initiate contact with the Data Fiduciary to continue the specified purpose for which their personal data was collected.

Processing of personal data of children/persons with disabilities:

The draft rules require Data Fiduciaries to implement appropriate technical and organizational measures to obtain verifiable consent from a parent or lawful guardian before processing the personal data of a child or a person with a disability. This consent must be obtained with due diligence, ensuring the identity of the parent or guardian is reliably confirmed. The verification process can be conducted by referring to either: the Data Fiduciary's own records of reliable identity and age information, or voluntarily provided identity and age details, or a virtual token that links to this information. Such virtual tokens may be issued by an authorized entity, such as a government agency or a Digital Locker service provider, ensuring that the information is verified and complies with Indian law.

The rules have also defined "**person with disability**" to mean and include individuals who experience long-term physical, mental, intellectual, or sensory impairments that, when interacting with various societal barriers, hinder their full and effective participation in society. Such individuals, despite receiving adequate support, are unable to make legally binding decisions. Furthermore, the definition includes individuals suffering from conditions such as autism, cerebral palsy, mental retardation, or a combination of these conditions, as well as those with severe multiple disabilities.

Additional obligations of SDFs:

The draft rules introduce additional obligations for SDFs to strengthen data protection practices. These obligations include:

DPIA and Audit:

A Significant Data Fiduciary is required to conduct an annual DPIA and data audit.

1. **Report Submission to the Board:** The entity responsible for conducting the DPIA and audit must submit a report to the Board, detailing significant findings and observations arising from the assessment and audit.
2. **Algorithmic Software Verification**: The Significant Data Fiduciary must exercise due diligence to ensure that any algorithmic software used for processing personal data—such as for hosting, display, transmission, or sharing—is not likely to infringe on the rights of Data Principals. This adds a layer of protection against potential misuse of automated processing, including in AI models.
3. **Data Localization and Restrictions:** The rules mandate that certain personal data, as specified by the Central Government based on recommendations from a designated committee, must be processed by the Significant Data Fiduciary within India's territorial boundaries. Additionally, any traffic related to the data flow must not be transferred outside the country, ensuring that critical data remains within Indian jurisdiction.

Rights of Data Principals:

The draft rules outline the responsibilities of Data Fiduciaries and Consent Managers to ensure Data Principals can effectively exercise their rights under the Act. Key provisions include:

Publication of Rights Exercise Mechanisms:

Data Fiduciaries, and where applicable, Consent Managers, must provide clear information on how Data Principals can exercise their rights. This should be published on their websites or apps and must include the available methods for requesting the exercise of rights, as well as any necessary particulars (e.g., usernames or identifiers) required for identifying the Data Principal under their terms of service.

1. **Request Process for Access and Erasure**: To access personal data or request its erasure, the Data Principal must make a request to the Data Fiduciary to whom they previously gave consent for processing. The request must be made using the specified means and providing the necessary particulars as published by the Data Fiduciary.
2. **Grievance Redressal System**: Data Fiduciaries and Consent Managers must also provide information about the grievance redressal system on their website or app. This system should include a specified period for responding to Data Principals' grievances. To ensure the system's effectiveness, appropriate technical and organizational measures must be implemented.
3. **Nomination Rights**: Data Principals have the right to nominate individuals in accordance with the Data Fiduciary's terms of service and applicable laws. They must use the means and furnish the necessary particulars for exercising this right, as specified by the Data Fiduciary.

The rule defines "identifier" as any sequence of characters used by the Data Fiduciary to identify the Data Principal. This includes customer identification numbers, application reference numbers, enrolment IDs, or license numbers that allow for identification within the system.

Transfer of personal data outside India:

Personal data processed by a Data Fiduciary in India or in connection with offering goods or services to Data Principals within India can be transferred to any foreign country or territory subject to specific requirements to be determined by the Central Government.

Data Protection Board:

The Central Government will form a Search-cum-Selection Committee to recommend candidates for the Chairperson and Members of the Board, with the Cabinet Secretary or the Secretary of the MeitY chairing it. The Board will operate digitally, conducting meetings with a one-third quorum, and decisions will be made by majority vote. In urgent cases, the Chairperson may take action subject to ratification. The Board can also make decisions via circulation. Appointments of officers and employees will be made with the Government's approval, with terms specified in the relevant schedules.

Calling for information from Data Fiduciary or intermediary:

The Central Government may require any Data Fiduciary or intermediary to provide information as specified in the Seventh Schedule of the Act. The required information must be submitted within the specified time period. If disclosure could affect India's sovereignty, integrity, or security, the Data Fiduciary or intermediary must obtain written permission from the authorized person before disclosing the information. This obligation is in line with Section 36 of the Act.

Section 36 states that the Central Government may, for the purposes of this Act, require the Board and any Data Fiduciary or intermediary to furnish such information as it may call for.

JSA Analysis

The Draft Rules, provide crucial operational guidelines for implementing the DPDPA.

The draft rules ensure that consent notices are clear and informative, empowering data principals to make informed choices. These notices must be independent of other information, presented in plain language, and include itemized descriptions of personal data, its purpose, and services provided. Additionally, data fiduciaries must include a link for

data principals to withdraw consent, exercise their rights, and file complaints with the Data Protection Board, simplifying the process of informed consent.

The rules also provide clarity on consent managers, establishing standards for entities wishing to register as consent managers with the Board, and outlining their responsibilities, including onboarding data fiduciaries, maintaining records, and ensuring compliance. This facilitates the creation of efficient consent management workflows.

Furthermore, the rules create accountability for the State or its departments processing personal data by prescribing the adherence to privacy principles like data minimization, purpose limitation, and security safeguards for government data processing.

While the draft rules specify that breach notifications must be sent 'without delay,' the absence of a clear timeline for notifying data principals creates operational uncertainty. On the other hand, the 72-hour deadline for detailed reporting to the Board is especially challenging, as it is a very short period and may pose significant operational challenges for organizations to investigate, assess, and document breaches and report with all the details.

In terms of children's data and persons with disabilities, the rules specify how parental/guardian consent must be verified, enhancing protections. For children, the identity of the parent providing consent must be verified through existing records with the data fiduciary, government-issued identification, or digital tokens such as those mapped to the Digital Locker service. However, the rules also introduce some exceptions to these requirements, by class of fiduciaries and purposes of processing. The purposes of processing for which exemptions are granted are generic, which could have an effect of diluting the protection afforded to vulnerable categories like children.

SDFs are subject to increased operational responsibilities, including annual DPIAs and data audits, reportable to the Board. Annual independent audits could add to the cost of compliance and operational challenges.

The draft rules impose an obligation on due diligence on an SDF to verify that any algorithmic software it deploys to process personal data is not likely to pose a risk to the rights of data principals. This is likely to impact an SDF employing AI in its products, processes or services to test the models against bias, unlawful personal data processing or threats and attacks. Interestingly, so far MeitY has only issued advisories to intermediaries and platforms to test their models and algorithms to ensure it does not permit discrimination, to give information to users on unreliability of outputs from models under testing and prohibiting users from using such models in contravention of the Information Technology Act and Rules. While the validity and enforceability of the MeitY advisories was under question, the draft rules could now codify this requirement of due diligence in legislation. This is an important step for AI governance.

Another curveball thrown by the draft rules is the data localization requirements for SDFs, which mandate that certain personal data be stored and processed within India's borders which would present operational challenges for companies that rely on global service delivery, distributed infrastructure and cloud-based services. These localization rules could lead to higher compliance costs and operational inefficiencies. The requirement to keep data within Indian borders also creates complexities in terms of data storage, management, and access control, potentially hindering business flexibility and global coordination.

DPDPA indicated that the Central Government may publish a list of countries/regions to which personal data cannot be transferred. The Rules, however, seem to provide a broader restriction on transfer of data outside India. The Rules now prescribe that the Central Government may specify certain restrictions for processing of personal data of data principals in India, outside India. These restrictions may apply to making personal data of individuals in India available to any foreign State, or to any person or entity under the control of or any agency of such a State.

Infotech Practice (Privacy and Data Protection)

Our team understands the importance of data privacy in today's digitally interconnected world. We have dedicated our practice to ensuring that your and your customers' personal and business data remains secure, compliant, and respects the sovereignty of individuals and jurisdictions globally.

We prioritise creating bespoke solutions tailored to your business needs. We recognise that every business has unique data privacy challenges, and we use our deep understanding of international and domestic regulations to provide you with the most effective and robust legal strategies. JSA provides advice on highly sophisticated data management, data security and privacy issues. Our depth of experience gives our clients the crucial advantage of consistent and comprehensive, yet practical advice. Our Technology Law Practice group has successfully worked with several multinational organisations for the structuring and roll-out of privacy and information-security programs. We have carried out audit and risk assessments, customised global privacy and information management policies, helped create international data transfer strategies, structure and negotiate complex international data transfer agreements.

This Compendium has been prepared by:

Akshaya Suresh
Partner

Aravindini Magesh
Associate

Drishya Kamath
Associate

18 Practices and
41 Ranked Lawyers

7 Ranked Practices,
21 Ranked Lawyers

12 Practices and 50 Ranked Lawyers

14 Practices and
12 Ranked Lawyers

20 Practices and
22 Ranked Lawyers

Ranked Among Top 5 Law Firms in India for ESG Practice

Recognised in World's 100 best competition practices of 2025

Among Top 7 Best Overall Law Firms in India and
11 Ranked Practices

---

11 winning Deals in
IBLJ Deals of the Year

---

11 A List Lawyers in
IBLJ A-List - 2024

Asia M&A Ranking 2024 – Tier 1

Employer of Choice 2024

Energy and Resources Law Firm of the Year 2024

Litigation Law Firm
of the Year 2024

Innovative Technologies Law Firm of the Year 2023

Banking & Financial Services
Law Firm of the Year 2022

Ranked #1
The Vahura Best Law Firms to Work Report, 2022

Top 10 Best Law Firms for Women in 2022

7 Practices and
3 Ranked Lawyers

For more details, please contact km@jsalaw.com

Ahmedabad | Bengaluru | Chennai | Gurugram | Hyderabad | Mumbai | New Delhi