cyril amarchand mangaldas

ahead of the curve

FAQs - The Digital Personal Data Protection Act, 2023

Disclaimer:

This Guide does not purport to be exhaustive or conclusive. It does not constitute a legal advice or opinion, and it should not be relied upon by any person for any purpose, nor is it to be quoted or referred to in any public document or shown to, or filed with any government authority, agency, or other official body without our consent. We are relying upon relevant provisions of the Indian laws in force, as on December 7, 2025, and the rules thereunder, and the judicial and administrative interpretations thereof, which are subject to change or modification by subsequent legislative, regulatory, administrative, or judicial action or decisions. No part of this report may be copied or re-distributed in any form without the prior written consent of Cyril Amarchand Mangaldas.

FAQ

These FAQs aim to provide an overview on the core elements and obligations under The Digital Personal Data Protection Act, 2023 and are structured into 5 (five) parts:

Assumption and Qualifications:

These FAQs are a thought leadership initiative, and do not constitute legal advice. Their contents are subject to evolving regulatory guidance, and contrary positions which may be taken by courts and regulators including the Ministry of Electronics and Information Technology and Data Protection Board.

They are not intended to be relied upon as legal advice, and we would urge that you review and validate any legal positions outlined before you apply them to your specific fact circumstances, and consult your relevant advisors before you implement them.

Introduction

In the landmark judgment of *Justice K.S. Puttaswamy (Retd.) v. Union of India,*[1] the Hon'ble Supreme Court of India recognized the right to privacy as a fundamental right protected under Article 21 of the Constitution of India, and mandated a robust data protection regime that improved on the current regime under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (**SPDI Rules**). After a prolonged multi-year consultative process and different iterations of what the new data protection law of India could look like, the Digital Personal Data Protection Act, 2023 (**DPDPA**) was enacted on August 11, 2023.

About DPDPA

DPDPA is India's first comprehensive legislation horizontal regulating the collection, processing, and protection of personal data (**PD**). It establishes a principle-based framework for processing of PD, intended to balance an individual's informational privacy rights and expectations with the legitimate needs of data processing. Some of the key objectives sought to be achieved with the implementation of DPDPA are:

- empowering individuals with increased autonomy and enforceable rights related to the processing of their PD;
- facilitating lawful, fair, and transparent data processing;
- imposing transparency and accountability obligations on entities collecting and using PD; and
- aligning India's data governance framework with global standards.

DPDPA introduces new concepts and requirements that will alter the manner in which PD is processed by private and public entities as well as state and its agencies. With material differences to SPDI Rules and unique concepts that do not have a global parallel, DPDPA is reliant on consent basis of processing, limits other alternative processing grounds, introduces new data protection rights, provides for setting up of a new quasi-judicial body, and proposes steep penalties.

Implementation

On November 14, 2025, the Central Government (**CG**) notified the Digital Personal Data Protection Rules, 2025 (**DPDP Rules**). DPDP Rules supplement the different norms under DPDPA and set out the operational framework for its implementation. Alongside, CG released timelines for implementation of DPDPA in a phased manner.

Marking the first phase of implementation, provisions defining different concepts, composition and functioning of the Data Protection Board (**DPB**), and those relating to administrative and rule-making powers were made effective immediately from November 14, 2025.

[1] Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1.

The second phase of implementation concerning eligibility and registration criteria, and roles and responsibilities of consent managers will be made effective after 12 (twelve) months i.e., November 14, 2026. The last and final phase of implementation will cover all substantive data processing obligations and data principal rights, and shall be made effective after 18 (eighteen) months i.e., May 14, 2027.

Part A: Key concepts and Scope

1. What is data and PD under DPDPA?

"Data" is defined as structured representation of information, facts, concepts, opinions or instructions that is suitable for communication, interpretation, or processing manually or using automated means (i.e., digital processing of data).[2]

"Personal Data" is defined as any data about an individual who is identifiable by or in relation to such data.[3]

While the definition is wide to include PD contained in digital and physical forms, Section 3(a) of DPDPA limits its applicability to the processing of digital PD i.e., any PD that is collected digitally, or subsequently converted into digital form.

For instance, details entered in a physical register or customer details collected through physical survey forms may not be construed as PD at the time of collection, but may be covered when subsequently digitized.

2. What is processing of PD?

"*Processing*" is defined to include all wholly or partly automated operation(s) performed on PD and includes all activities performed on PD such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, indexing, combination, sharing, disclosure, dissemination, etc. Essentially, any dealing with PD is processing, and the entire processing lifecycle of PD is covered.

3. Who are data principals, data fiduciaries, and data processors?

- **Data Principal** - the individual to whom PD relates to (akin to data subject) and includes, in case of (i) children up to age of 18 (eighteen) years (**Minor**), their parents or lawful guardian; (ii) persons with disabilities (**PWDs**), their lawful guardian; and (iii) death or incapacitation of the individual, their nominee;
- **Data Fiduciary** - the person or entity who alone or in conjunction with others, determines the means and purposes of processing (akin to data controller); and
- **Data Processor** - the person or entity that processes PD for the Data Fiduciary.

[2] Section 2(h) of DPDPA.
[3] Section 2(t) of DPDPA.

Similar to Singapore PDPA and Hong Kong PDPO, all obligations and liabilities emanating under DPDPA are directly applicable to Data Fiduciaries, who must ensure that engaged Data Processors are contractually obligated or otherwise are required to comply with DPDPA's requirements.[4]

For instance, when a Data Principal exercises her right to withdraw consent, the Data Fiduciary is obligated to erase her PD (unless extended retention is permissible under DPDPA or applicable law) and also ensure deletion by its engaged Data Processors.[5]

4. Does DPDPA provide for joint fiduciaries and sub-processors?

Unlike the EU GDPR that expressly provides for joint controllers and sub-processors, DPDPA does not explicitly refer to joint Data Fiduciaries or sub-processors.

However, the definitions of Data Fiduciary and Data Processor can be read to include (i) joint Data Fiduciaries when the processing purposes and means have been decided collectively/jointly by more than one Data Fiduciary; and (ii) sub-processors where the primary Data Processor engages a step-down Data Processor to process PD on behalf of the Data Fiduciary.

5. What is the territorial scope of DPDPA?

DPDPA governs all processing of digital PD within India.[6] It also applies extra-territorially to processing of digital PD outside of India, where undertaken in connection with activity related to offering of goods or services to Data Principals within India (**Long-Arm Application**),[7] even where the Data Fiduciary or Data Processor has no physical location or legal presence in India. For instance, processing of PD by a global airline that does not have any presence in India to provide services in India is likely to be covered under DPDPA through Long-Arm Application.

DPDPA will also regulate processing of PD of non-Indians who are physically located in India.

6. Does DPDPA apply to anonymised and pseudonymised data?

DPDPA does not expressly exempt its application to anonymised or pseudonymised data.

Anonymisation is typically understood as the irreversible process of transforming or converting PD into a form in which the individual cannot be identified. Consequently, and relying on the scope of DPDPA, anonymised data is likely to be outside DPDPA's purview. While there are no globally accepted standards for anonymisation, some of the widely used techniques include randomization[8] and generalization.[9]

Pseudonymisation or deidentification is commonly understood as the process of removing, masking, replacing, or segregating identifiers from PD in such manner that the output data on its own does not

[4] Section 8(1) of DPDPA.
[5] Section 8(7) of DPDPA.
[6] Section 3(a) of DPDPA.
[7] Section 3(b) of DPDPA.
[8] Randomization generally refers to various techniques that alter the veracity of data in order to remove the strong link between the data and the individual, and involves techniques such as noise addition, permutation, and differential privacy.
[9] Generalization typically involves techniques that generalize or dilute the individual identification attributes by modifying the respective scale or order of magnitude, such as aggregation, k-anonymity, and l-diversity.

directly result in identifying the concerned individual. Thus, it is different from anonymisation, and when combined with identifiers or linked with other data sets, can result in the identification of the individual. Hence, pseudonymised data is likely to remain within DPDPA's ambit.

7. Is processing of publicly available PD regulated under DPDPA?

DPDPA excludes from coverage completely, all PD that is:

- made publicly available (such as through public profiles) by the data principal, or
- becomes public through the operation of law (such as public government records)

While this is the broadest public data exception globally, it does not mean that all "publicly available" PD stands unregulated. Before relying on "public" data, it may be advisable to make sure that the PD is indeed public and meets one of the two tests above.

8. What are the exclusions to DPDPA's application scope?

Apart from anonymised data and public data as discussed at FAQ# 6 and 7 above, DPDPA also excludes from its ambit, processing of PD:

- by an individual for any personal or domestic purpose;
- by state bodies as may be notified by the CG as well as subsequent processing of such PD by CG in the interest of sovereignty and integrity of India, state security, friendly relations with foreign states, maintenance of public order, or preventing incitement to any cognizable offence relating to the foregoing; and
- for research, archiving, or statistical purposes, if the PD is not processed to make any specific decision concerning the DP, processing is necessary, and such processing is performed in accordance with standards prescribed under the Second Schedule of DPDP Rules (*discussed in FAQ [23] below*).

Additionally, DPDPA empowers the CG to notify Data Fiduciary(ies) who would be exempted from DPDPA compliance. Such notification can be issued before the expiry of 5 (five) years from DPDPA commencement date (collectively referred as **Exclusions**).

Further, please note that DPDPA also provides for several exemptions that stand to benefit Data Fiduciaries, and these are discussed subsequently.

9. Does DPDPA define sensitive personal data?

No, DPDPA does not classify PD into non-sensitive and sensitive data as currently provided for under SPDI Rules.[10]

[10] Rule 3 of SPDI Rules define "sensitive personal data" to include passwords, financial data, health data, biometrics, sexual orientation, and any details relating to the foregoing categories.

However, in practice, certain PD sets may call for higher degree of protection as compared to others. To this effect, DPDPA makes reference to "sensitivity" of PD as a relevant factor for classification of certain Data Fiduciaries as Significant Data Fiduciaries (**SDFs**),[11] and further, provides for type of PD involved in a breach scenario as a consideration for determining penalties.[12]

10. Who are significant data fiduciaries under DPDPA?

DPDPA empowers the CG to notify any Data Fiduciary or class of Data Fiduciaries as SDFs.[13]

While determining SDFs, the CG will base its assessment on various factors including (i) the volume and sensitivity of PD processed; (ii) risk to rights of Data Principals; (iii) potential impact on sovereignty and integrity of India; (iv) risk to electoral democracy; (v) security of state; and (vi) public order.

It is recommended that entities who meet some or all of these criteria, or whose processing activities otherwise carry high systemic risk anticipate classification as SDFs.

Upon notification, SDFs will be subject to additional obligations such as undertaking data protection impact assessment (**DPIA**), completing periodic audits, and appointing Data Protection Officer (**DPO**) as elaborated subsequently.

11. Can a company be a Data Fiduciary and Data Processor at the same time?

The distinction between Data Fiduciary and Data Processor is dependent on who has decided the means and purposes of processing. The definitions are purpose-specific and not entity-specific. Accordingly, the same organization, in relation to the same set of PD, may be a Data Fiduciary and Data Processor by processing it for different purposes.

For instance, where a KYC service provider is engaged by an organization for KYC purposes, the engaged third party can process PD as is necessary for the limited purpose of KYC verification and will be a Data Processor. Any other processing purposes solved by such processing, which is a purpose determined by the KYC service provider, including compliance with applicable laws or reuse of KYC data across multiple clients, is likely to make the KYC service provider an independent Data Fiduciary with respect to such purposes.

12. Where PD is collected physically but later stored online, is the digital storage covered under DPDPA?

Processing is defined widely to cover the entire lifecycle from collection to deletion of PD. As storage is a form of processing and in the given context, PD although collected physically is digitized for storage, it will be regulated as per DPDPA including determining the apt processing basis for storage and in line with retention and erasure obligations under DPDPA.

[11] Section 10(1) of DPDPA.
[12] Section 33 (2) of DPDPA.
[13] Section 2(z) of DPDPA.

13. What are the permissible processing bases under DPDPA?

Processing of PD can be undertaken only for lawful purposes (i.e., purposes not forbidden under law), either:

- with consent of Data Principal for specific purposes; or
- for certain legitimate uses (collectively referred to as **Processing Bases**) unless such processing is pursuant to an Exclusion or Exemption provided under DPDPA.

Part B: Consent Basis for Processing

14. What is a valid consent?

Consent is the key basis on which PD can be processed under DPDPA, and the thresholds contemplated for valid consent are significantly higher than those currently prevalent under the SPDI Rules.

Under DPDPA, a valid consent must be free, specific, informed, unconditional, unambiguous, and expressed through a clear affirmative action. Once granted, it must be withdrawable by the Data Principal with ease that is comparable to the ease with which it was obtained.[14]

Consent must be collected by providing a Notice for Consent (see below).

15. How can consent be obtained?

Prior to or at the time of obtaining consent, the Data Fiduciary is obligated to provide a notice requesting consent of the Data Principal (**Notice for Consent**). This notice must:[15]

- be in clear and plain language;
- be presented and understandable independently of any other information that has been or may be made available to the Data Principal;
- be accessible to Data Principal in English or any other language specified in the Eighth Schedule of the Constitution of India (**Official Languages**);
- provide a fair account of details necessary for Data Principal to provide informed and specific consent;
- in the minimum, provide for (i) itemised description of PD; (ii) the specified purposes and specific description of goods/services to be provided or uses to be enabled through processing of PD; and (iii) the particular communication link to access Data Fiduciary's website / application or both and a

[14] Sections 6(1) read with 6(4) of DPDPA.
[15] Sections 5(1) and 6(3) of DPDPA read with Rule 3 of DPDP Rules.

description of other means that Data Principal can use for withdrawing their consent, or exercising their rights, and complain to DPB; and

- should include contact details of the Data Fiduciary's authorised personnel who is responsible for communicating with the Data Principal who could be the grievance officer, or DPO in case of SDFs.

DPDP Rules do not provide for any format or template and are silent on relevant inclusions that would provide "fair account of details" to the Data Principal. While this creates ambiguity, it also leaves flexibility for businesses to determine the layout and additional content that they consider relevant for obtaining informed and specific consent. Consent must be signified through an affirmative action. Accordingly, mechanisms like pre-ticked boxes and implied consent language such as "*By continuing to use the application, you consent to processing of your PD*" may no longer be feasible under DPDPA.

16. What are the consequences of consent withdrawal?

The Data Principal is responsible for the consequences emanating from consent withdrawal. So, where processing of PD is required for providing goods or services and consent for processing has been withdrawn, the Data Fiduciary is no longer responsible to provide the offerings.[16]

Except where retention and continued processing of PD is permitted on other Processing Bases or is required for compliance with applicable law including DPDPA, upon withdrawal of consent, the Data Fiduciary must stop further processing and erase PD from its systems and require such cessation and erasure by its Data Processors as well.[17]

17. When does the obligation to obtain verifiable consent trigger and how to obtain such verifiable consent?

Subject to certain exemptions as provided in Fourth Schedule of DPDP Rules, Data Fiduciaries are required to obtain verifiable consent prior to processing of PD of Minors and PWDs. Such verifiable consent should be obtained from parents or lawful guardian for Minors, and that of lawful guardian in case of PWDs.

DPDP Rules prescribes the manner in which verifiable consent can be obtained. In context of Minors,[18] Data Fiduciary shall use technical and organizational measures for verification of the parent/lawful guardians' identity against reliable identity and age details that may be already available with the Data Fiduciary (such as identity information of the parent who already has an user account with the Data Fiduciary), or as voluntarily provided by parent/lawful guardian (akin to self-declaration), or through use of virtual tokens issued by the authorized entities that include using details or tokens verified and made available by a Digital Locker service provider.

In case of PWDs,[19] the Data Fiduciary must exercise due diligence to verify whether such guardian has been appointed by a court or law, or designated authority or committee, under the laws of guardianship.

[16] Section 6(5) of DPDPA.
[17] Section 6(6) of DPDPA.
[18] Rule 10(1) of DPDP Rules.
[19] Rule 11(1) of DPDP Rules.

18. Who are exempted from the obligation to obtain verifiable consent?

Certain Data Fiduciaries as provided in Fourth Schedule of DPDP Rules are exempted from the obligation to obtain verifiable consent, subject to adherence to stipulated conditions therein. These include clinical establishments, mental health establishments, healthcare professionals (like registered medical practitioners), allied healthcare professionals (like healthcare workers), educational institutions, individuals at creche and child day care centres, and transportation partners engaged by educational institutions are exempted from the obligation to seek verifiable consent.

However, the exemptions are limited in scope and valid only for certain processing purposes such as processing that is necessary and broadly restricted to providing health services, support healthcare treatment, and tracking and behavioural monitoring of Minors at educational institution, creche, day care centre, or during the course of transportation.

19. Who is a consent manager and what is likely to be witnessed under Consent Management framework?

The concept of "consent manager" is unique to DPDPA. Consent managers are intended to serve as a single point of contact, enabling data principals to provide, review, manage and withdraw their consent. Subject to qualification criteria and conditions around operations as prescribed in First Schedule to DPDP Rules, consent managers are obligated to register with DPB and operate an interoperable platform that maintains transparency and accessibility features for Data Principals.

DPDP Rules provides detailed qualification criteria and obligations for consent managers, some of which are indicated below.[20] It *inter alia* provides that an Indian company with net worth of minimum INR 20 million, with sufficient capabilities (including technical, financial, and operational), valid certifications for consent management platform, and good governance practices can seek registration as a consent managers with DPB. Further, it provides that consent management framework should onboard both Data Principals and Data Fiduciaries, function in a data blind fashion in the best interest of the Data Principal in a fiduciary capacity without outsourcing any of its obligations, and ensure that the offered consent management platform is as per standards and assurance framework as may be prescribed by DPB.

20. Is it mandatory for all organizations to appoint a consent manager?

No, it is not mandatory for all Data Fiduciaries to appoint a consent manager.

[20] Rule 4 read with First Schedule of DPDP Rules.

Part C: Alternative Bases for Processing

21. What are the legitimate use bases of processing?

Under DPDPA, Data Fiduciaries can process PD for certain "legitimate uses" without consent.[21] This covers processing personal data (**Legitimate Use Bases**):

- for a purpose for which the Data Principal has voluntarily provided their PD;
- for employment related purposes, or for safeguarding the employer from loss or liability like on account of corporate espionage or breach of confidentiality obligations, or for providing a benefit/ service to the employee;
- to comply with a judgment, decree or order under applicable law, or any order relating to contractual or civil matters under foreign law;
- to respond to a medical emergency involving a threat to the life or immediate threat to the Data Principal or someone else's health;
- to enable medical treatment or health services to a person during any epidemic, outbreak of disease or any other threat to public health;
- to ensure the safety of, or to assist any individual during a disaster or breakdown of public order; and
- by the state for delivery of subsidies, benefits, licenses, or services, where the data principal previously consented to processing of their personal data for such purpose or their personal data is already existing in government databases.

22. Are there any exempted processing scenarios where a Data Fiduciary can process PD without consent or any legitimate use?

Apart from the Processing Bases, the Data Fiduciary can process PD without consent or legitimate use under the following processing scenario:[22]

- where processing is necessary for enforcing any legal right or claim;
- processing of PD of a Data Principal located outside India pursuant to a contract entered between an Indian Data Fiduciary or Data Processor as one party and any person outside India as the other contracting party such as provision of cloud storage services to a foreign company when they store PD of their foreign employees in India;
- where processing is necessary for a court-driven corporate restructuring such as for NCLT approved merger, demerger, and amalgamation like disclosure of PD of key employees for implementing NCLT approved amalgamation;

[21] Section 7 of DPDPA.
[22] Section 17 of DPDPA.

- processing for purposes of ascertaining financial information, and assets and liabilities of any person having availed a credit facility from a financial institution;
- processing that is essential for the discharge of judicial, quasi-judicial, supervisory, regulatory function by a court, tribunal, or any other legally authorised body; and
- processing in the interest of prevention, detection, investigation, or prosecution of any offence or contravention of any applicable Indian law (collectively referred to as **Exemptions**).

Additionally, accounting for the nature and volume of PD processed, CG may notify Data Fiduciaries or classes thereof as exempted entities.

23. What are the compliances for processing PD to undertake research, archiving, and statistical activities?

Processing of PD for research, archiving, and statistical purposes is exempted under the DPDPA, provided it is (i) necessary for the mentioned purposes; (ii) not used to take any decision specific to the Data Principal; and (iii) carried out as per prescribed standards.

The following standards are prescribed under Second Schedule of DPDP Rules:

- processing is carried out in a lawful manner and be limited to such PD as is necessary for the underlying purposes;
- reasonable efforts are made to ensure the completeness, accuracy, and consistency of PD processed;
- retention is limited to durations that are needed to achieve the purposes, or for compliance with applicable laws;
- reasonable security safeguards are built in to prevent Personal Data Breach including one that involves Processor’s ecosystems;
- there is allocation of responsibility and accountability on persons who are Data Fiduciaries; and
- appropriate technical and organizational measures are implemented to effectively comply with the above stipulations.

Part D: Obligations and rights of Data Fiduciaries, Data Processors, and Data Principal

24. What are the key obligations of Data Fiduciaries under DPDPA?

All obligations under DPDPA and its consequent liability lie with the Data Fiduciary. In addition to the core obligation of ensuing that processing is only for lawful purposes with a valid Processing Bases, some of the other key obligations for Data Fiduciaries include:[23]

[23] Section 8 of DPDPA.

- engaging Data Processors only through a valid contract;
- ensuring the accuracy, completeness, and consistency of PD processed where PD is likely to be used for making a decision concerning the Data Principal or where PD is disclosed to another Data Fiduciary;
- implementing appropriate technical and organizational measures for processing of PD in compliance with DPDPA;
- implementing reasonable security measures for preventing Personal Data Breach;
- notifying the DPB and Data Principals in case of a Personal Data Breach;
- erasing PD and causing engaged Data Processors to erase PD processed by them for the Data Fiduciary, upon withdrawal of consent if consent is the Processing Basis, or once the processing purposes are achieved, whichever is earlier, except where extended retention period is necessary for compliance with applicable law.

25. With respect to retention and erasure, what are the specific stipulations under DPDPA?

PD must be erased once the specified purpose is no longer being served or upon withdrawal of consent.[24] Retention beyond the specified period is permitted only if it is required for compliance with applicable laws, and/or necessary for dispute resolution or regulatory investigations.

26. Is the 1-year retention period mandatory for all organizations? What happens when different retention timelines are mandated under other laws?

Rule 8(3) of DPDP Rules obligate every Data Fiduciary and its Processors to retain PD processed along with associated traffic data and processing logs for a minimum period of 1 (one) year from the date of processing for the purposes mentioned in the Seventh Schedule of DPDP Rules i.e., use by the state or any of its instrumentalities for sovereignty, security, and integrity of India, or for performance of any function under law as directed by authorized person under such law, or for aiding state's assessment for SDF notification by MeitY. After this duration, Data Fiduciary and its Processors must erase PD and its associated details unless prolonged retention is required under applicable laws.

Hence, the 1-year retention is mandatory for all organizations. Where another applicable law (or the Third Schedule of DPDP Rules) requires longer retention, such longer period will prevail over the minimum 1 year duration.

27. What is the mandatory retention requirement under Third Schedule of DPDP Rules?

Section 8(7) of DPDPA obligates every Data Fiduciary to erase PD unless retention is required for compliance with applicable law, either upon withdrawal of consent by the Data Principal, or as soon as it is reasonable to assume that the specific purpose is no longer served, whichever is earlier.

[24] Section 8(7) of DPDPA.

Elaborating on when it is reasonable to assume that the specific purpose is no longer served, Section 8(8) of DPDPA states that such assumption is viable when the Data Principal has not approached the Data Fiduciary for performance of the specific purpose and has not exercised any rights in relation to such processing for the prescribed durations as notified for different classes of Data Fiduciaries (**Disengagement Criteria**).

Rules 8(1) and (2) read with Third Schedule of DPDP Rules provide the Disengagement Criteria for certain kinds of Data Fiduciaries in relation to identified purposes and the corresponding retention period therein, after the expiry of which such Data Fiduciaries must assume disengagement and proceed with erasure by providing a 48 (forty-eight) hours' notice to the concerned Data Principal as a confirmatory exercise before deletion, unless prolonged retention is required due to other applicable law. The covered Data Fiduciaries, identified purposes, and retention periods under Third Schedule are as follows:

- Covered Data Fiduciaries are e-commerce entities and significant social media intermediaries with minimum 20 (twenty) million, and online gaming intermediaries with minimum 5 (five) million registered users in India;
- Identified purposes are for enabling the user's access to their account or to any virtual token that is issued by or on behalf of the Data Fiduciary and is stored on the platform of the covered Data Fiduciaries and can be used to get money, goods or services; and
- PD that is required for the identified purposes must be retained for 3 (three) years from the date of commencement of DPDPA or the date on which the user last reached out to the covered Data Fiduciaries for the identified purposes, whichever is latest.

28. How can Data Fiduciaries ensure compliance with DPDPA by its Data Processors?

The Data Fiduciary may engage a Data Processor through a valid contract. Hence, depending on factors such as sensitivity of processing, technology used, nature of PD processed and purposes of processing, a Data Fiduciary should evaluate signing a detailed data processing agreement or include suitable covenants in the main contract with specific obligations to comply with DPDPA. DPDP Rules further require that the contract executed between Data Fiduciary and Data Processor shall include appropriate provisions for taking reasonable security safeguards.[25] Additionally, Data Fiduciaries should retain audit and information seeking rights to monitor actual processing activities and assessing compliance with DPDPA.

29. What are the additional obligations for SDFs?

Additionally, SDFs are required to comply with the following:

- appoint an India-based DPO who is accountable to the board of directors and serve as the grievance redressal point of contact;[26]

[25] Rule 6(1)(f) of DPDP Rules.
[26] Section 10(2)(a) of DPDPA.

- appoint an independent auditor to conduct periodic audits;[27]
- conduct periodic DPIAs and audits, and here before DPDP Rules propose a yearly frequency with an initial DPIA and audit exercise completed within 12 (twelve) months of being notified as an SDF;[28]
- exercise due diligence to ensure deployed algorithmic software does not pose risk to Data Principals' rights;[29] and
- comply with standards relating to cross border transfers, if and when they are specified by a CG committee.[30]

30. Who can be DPO?

SDFs are obligated to appoint DPO, who shall represent the SDF for DPDPA purposes. Section 10 requires a DPO to be an Indian resident, who (i) is responsible and accountable to the governing body of the SDF (such as board of directors of a company), and (ii) acts as the point of contact for grievance redressal processes under DPDPA.

No other qualitative criteria or guidance is provided under DPDPA or DPDP Rules but as DPO is responsible for DPDPA compliance, it is advisable that appointed DPO has suitable expertise and skillsets including legal, technical, and governance to fulfil their roles and responsibilities.

31. What are the rights of Data Principals under DPDPA?

DPDPA provides for the following rights to Data Principals:

- right to nominate a nominee to act on their behalf upon death or incapacitation;[31]
- right to seek grievance redressal;[32] and
- right to reach out to DPB.[33]

Further, where PD is processed on Consent or voluntary submission basis, the Data Principal has the following rights with respect to processed PD:

- access information about PD being processed and shared;[34] and
- seek correction, completion, updation, and erasure of PD.[35]

Furthermore, only where Consent is the basis, the Data Principal has the right to withdraw consent[36] and appoint a consent manager as its single point of contact.[37]

[27] Section 10(2)(b) of DPDPA.
[28] Section 10(2)(c) of DPDPA read with Rule 13 of DPDP Rules.
[29] Rule 13(3) of DPDP Rules.
[30] Rule 13(4) of DPDP Rules.
[31] Section 14 of DPDPA.
[32] Section 13 of DPDPA.
[33] Sections 5(1)(iii) and 5(2)(iii) of DPDPA.
[34] Section 11 of DPDPA.
[35] Section 12 of DPDPA
[36] Section 6 of DPDPA.
[37] Section 6(7) of DPDPA.

Part E: Miscellaneous

32. What constitutes reasonable security safeguards for protecting PD under DPDPA?

Unlike SPDI Rules that recognized compliance with international standards such as ISO/IEC 27001 as deemed compliance with the obligation to implement reasonable security measures, DPDPA does not refer to any such standards. What would constitute "reasonable" is likely to depend on the nature and sensitivity of processing, the kind of PD processed, the likely impact on Data Principal where a Personal Data Breach occurs, and other such factors.

To this effect, DPDP Rules emphasize on appropriate technical and organizational measures such as data security covenants in data processing agreements, and provide for preventive measures like encryption, obfuscation, making, access controls alongside breach response mechanism such as logging and detection measures. Further and in order to enable breach identification, investigation, and remediation, DPDP Rules propose maintenance of logs and relevant PD for at least 1 (one) year.[38]

33. What is a Personal Data Breach?

Personal Data Breach is defined under DPDPA as any unauthorized processing of PD or its accidental disclosure, acquisition, sharing, use, alternation, destruction or loss of access to PD, that compromises the confidentiality, integrity, or availability of PD.

34. What types of Personal Data Breaches must be notified to DPB and Data Principals?

All kinds of Personal Data Breach that involve unauthorised processing and have resulted in compromising the confidentiality, integrity, and availability of PD must be reported to DPB and the concerned Data Principals. Notably, this requirement is a departure from several global laws such as EU GDPR that require notification to data subjects depending on severity of the breach involved.

35. What information must be included in a Personal Data Breach notification and what are the timelines?

DPDP Rules mandate a three-tier Personal Data Breach notification requirement as follows:[39]

- Upon occurrence of a Personal Data Breach, the Data Fiduciary must immediately notify basic details about the breach such as nature, time, location and likely impact to DPB.
- Further, it must immediately notify Data Principals about nature, time, location of breach, likely consequences, mitigation steps, recommended safety measures, and contact details for queries.
- Thereafter and within 72 (seventy-two) hours or such extended period as may be permitted, the Data

[38] Rule 6 of DPDP Rules.
[39] Rule 7 of DPDP Rules.

Fiduciary must submit a detailed report with DPB which includes details about nature and extent of breach, mitigation measures, responsible parties, root cause analysis, and proof of notifications sent to affected Data Principals.

36. What are the cross-border PD transfer restrictions under DPDPA?

Subject to compliance with DPDPA, PD can be transferred outside India to other jurisdictions, except those jurisdictions that are prohibited by CG through notification.[40] DPDP Rules further propose that CG can, through notification, restrict the ability of SDFs to transfer specific types of PD outside of India.[41]

37. What are the penalties for non-compliance with DPDPA?

The following penalties are prescribed for Data Fiduciaries under DPDPA; up to:

- INR 2500 (two thousand five hundred) million for failing to implement reasonable security safeguards;
- INR 2000 (two thousand) million for not notifying the DPB or affected Data Principals of a Personal Data Breach;
- INR 2000 (two thousand) million for violating obligations related to processing of PD of Minors; and
- INR 1500 (one thousand five hundred) million on SDFs where they are in breach of their additional obligations.

Additionally, the DPB may impose penalty of up to INR 500 (five hundred) million for any other breach. Moreover, Data Principals may face penalties up to INR 10,000 (ten thousand) for failing to observe their duties.

The DPB is obligated to provide show-cause before imposing penalty, and while determining penalty, is likely to consider various factors such as (i) severity, duration, and nature of the breach; (ii) the type of PD affected; any gains or losses incurred; (iii) mitigation efforts; and (iv) the likely impact of the imposition of the penalty.

38. Are there technology enabled solutions that businesses could use for compliance with DPDPA?

Compliance with the requirements under DPDPA is an ongoing exercise and technology enabled solutions play a crucial role. Several key compliances around consent, honoring Data Principal's rights, redressal of their grievances, maintaining data inventory, and implementing reasonable security measures are facilitated through technology tools. These include use of privacy enhancing tools, commonly known as PETs (such as homomorphic encryption, differential privacy, federated learning, and communication anonymizers), consent management dashboards, data subject access rights (DSARs), and other privacy

[40] Section 16(1) of DPDPA.
[41] Rule 13 of DPDP Rules.

information management system (PIMS) tools. While necessity of using such solutions will depend on a variety of factors including existing digital footprint, user base, volume of PD processed, nature of processing undertaken, number of right requests and grievances received, it is likely that organizations that are data intensive will require technological enablers to remain DPDPA compliant more than others. However, organizations should note that technology acts only as an enabler and does not substitute compliance with core statutory requirements such as purpose limitation, obtaining a lawful Processing Basis, accuracy, and accountability.

39. What happens where a platform user does not respond to an organization's request and notice for consent?

Given that consent must be signified through an affirmative action of the Data Principal, processing of PD of a platform user on the basis of consent where they remain unresponsive to the platform's request for consent relying on their continued use of the platform may not be permissible, unless such processing can be substantiated on other Alternative Processing Bases or covered under the available Exemptions and Exclusions. For instance, companies are required to maintain logs of their information and communication technology systems for a rolling period of 180 (one hundred and eighty) days pursuant to the Directions issued by CERT-In dated April 28, 2022 under Section 70B(6) of the Information and Technology Act, 2000, relating to information security practices, procedure, prevention, response and reporting of cyber incidents (**CERT-In Directions**) and a platform operator may rely on compliance with law basis to justify its collection and retention of technical information about user's session on the platform. However, in all such cases, the underlying purposes are limited and caution has to be exercised to ensure that processing undertaken is necessary and limited following the principles of data minimization, purpose limitation, and storage limitation.

40. Who is responsible for collecting consent when PD is collected by the Processor for the Data Fiduciary?

All obligations under DPDPA apply to Data Fiduciaries, and they are obligated to ensure that their engaged Processors remain compliant with DPDPA. Where a Data Fiduciary engages a Processor to directly collect PD from Data Principal such as collecting feedback of Data Principals through surveys and market studies, the Data Fiduciary must provide its Notice for Consent and obligate the Processor to obtain DPDPA compliant consent before collecting PD. Where Data Principal refuses to signify their consent, the Processor should not collect any PD, unless the Data Fiduciary has permitted collection on any other permissible Processing Bases.

Glossary

Abbreviation	Description
AI	Artificial Intelligence
BRD	Business Requirements Document for Consent management under DPDPA released by MeitY
CG	Central Government
DPB	Data Protection Board
DPDPA	Digital Personal Data Protection Act, 2023
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DPDP Rules	Digital Personal Data Protection Rules, 2025
GDPR/ EU GDPR	General Data Protection Regulation, 2018 of the European Union
Hong Kong PDPO	Personal Data (Privacy) Ordinance, 1995 of Hong Kong
INR	Indian Rupees
ISO/IEC 27001	International Organization for Standardization/International Electrotechnical Commission 27001
MeitY	Ministry of Electronics and Information Technology
Minor	Children up to the age of 18 years
NCLT	National Companies Law Tribunal
PD	Personal Data
PWD	Persons with Disabilities
SDF/SDFs	Significant Data Fiduciaries
SPDI	Sensitive personal data or information as defined under the Rule 3 of SPDI Rules, that is, personal information about a person relating to passwords; financial information (such as details of bank accounts, credit and debit card or other payment instrument); physical, physiological and mental health condition; sexual orientation; medical records and history; and biometric information
SPDI Rules	Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
Singapore PDPA	Personal Data Protection Act, 2012 of Singapore

Key Contacts

Arun S. Prabhu
Partner
(Co-Head – Digital | TMT)
arun.prabhu@cyrilshroff.com

Mihir Rale
Partner
(Co-Head – Digital | TMT)
mihir.rale@cyrilshroff.com

Huzefa Tavawalla
Partner
(Head – Digital Disruption)
huzefa.tavawalla@cyrilshroff.com

Arya Tripathy
Partner
arya.tripathy@cyrilshroff.com

Anirban Mohapatra
Partner
anirban.mohapatra@cyrilshroff.com

Contributors

Arun S. Prabhu
Partner
(Co-Head – Digital | TMT)

Arya Tripathy
Partner

Apoorva Sundar
Principal Associate

Dylan Sharma
Associate

Tannvi R
Associate

Yaqoob Alam
Associate

Milind Yadav
Associate

www.cyrilshroff.com
www.cyrilshroff.com/blogs

mumbai
Peninsula Chambers, Peninsula Corporate Park, GK Marg,
Lower Parel, Mumbai – 400 013, India
T +91 22 6660 4455
E cam.mumbai@cyrilshroff.com

delhi-ncr
Level 1 & 2, Max Towers, C-001/A, Sector 16 B,
Noida – 201 301, Uttar Pradesh, India
T +91 120 669 9000
E cam.delhi@cyrilshroff.com

ahmedabad
Block A-1512, 15th Floor, Navratna Corporate Park,
Ambli Bopal Road, Bodakdev, Ahmedabad – 380 058, India
T +91 79 3503 9999
E cam.ahmedabad@cyrilshroff.com

bengaluru
3rd Floor, Prestige Falcon Tower, 19, Brunton Road,
Off M G Road, Bengaluru – 560 025, India
T +91 80 6792 2000
E cam.bengaluru@cyrilshroff.com

presence also in hyderabad, chennai, gift city, singapore and abu dhabi

cyril amarchand mangaldas
ahead of the curve