Digital Personal Data Protection Rules (2025)

January 2025

pwc

01

Overview of draft DPDP rules 2025

Key tenets of the DPDP rules

01

Rights of Data Principals:
Data Fiduciaries and Consent Managers must clearly outline on their website or app the process for Data Principals to exercise their rights under the Act, including the Data Principal's right to nominate.

02

Data privacy notice and consent:
Notice should include an itemised list of collected personal data, the purpose for processing it, and itemised description of goods and services provided. It should also include a link to access the website or app to withdraw consent and make a complaint to the Data Protection Board.

03

Verifiable parental consent:
For a Data Principal under 18 or any person with a disability, the Data Fiduciary must obtain verifiable consent from the parent or guardian.

04

Reasonable security safeguards:
Data Fiduciaries must protect the personal data of their Data Principals by taking adequate data security measures.

05

Data privacy breach notification:
In case of a data breach, the Data Fiduciary should notify affected Data Principals and the board within 72 hours.

06

Personal data deletion:
For specific scenarios, the personal data of Data Principals who have not interacted with the Data Fiduciary for three years must be deleted, and they should be notified of the same at least 48 hours before deletion.

Key tenets of the DPDP rules

07

Obligations of Significant Data Fiduciaries (SDFs):
SDFs must conduct an annual Data Protection Impact Assessment (DPIA) and data privacy audits.

08

Cross-border data transfer:
Data Fiduciaries processing data in India or providing goods or services from outside India must adhere to any requirements established by the central government regarding the availability of such personal data to a foreign state or its entities.

09

Exemptions to the act:
Data Fiduciaries like healthcare professionals, educational institutions and childcare providers are exempt from certain provisions regarding children's data, but can only process it for specific activities (e.g. safety monitoring and transportation tracking).

10

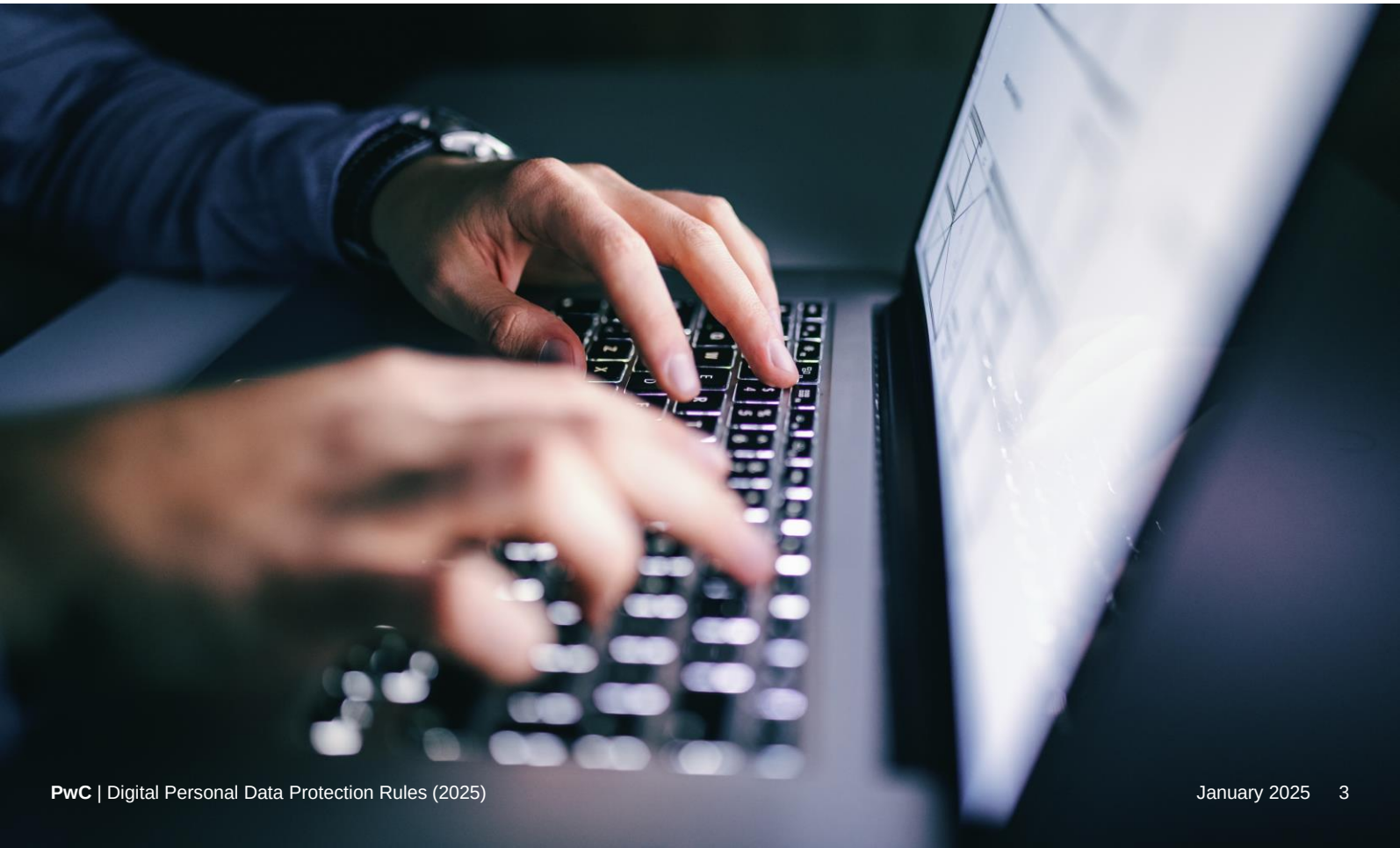
Publishing the details of the DPO or representative:
Data Fiduciaries should display the contact details of any designated person such as the data protection officer (DPO).

11

Consent Manager:
Must be an Indian-incorporated company with a net worth of at least INR 2 crore and a certified interoperable platform for managing consent.

12

Processing of personal data by the State:
The State and instrumentalities may process the personal data of individuals to provide various benefits, services, certificates, licences or permits, as permitted by laws and policies, or through public funds.



Our perspective on key tenets

Reference to the act	Requirement in the act	Proposed rules	Our perspective
Chapter II, Section 5 - Notice	The notice for consent-based processing should be served to: • new and existing Data Principals as soon as it is reasonably practicable. The notice should contain details about: • personal data and the purpose of processing • the manner to exercise rights • the manner to make a complaint to the board. The notice should be accessible in English, or any language specified in the Eighth Schedule of the Constitution of India.	**Rule 3** The notice from the Data Fiduciary to the Data Principal should: • be independently understood • have clear and plain language • provide a fair account of the details such as: a) an itemised list of personal data b) specified purpose of processing and itemised description of goods and services to be provided c) communication link for accessing the website or app or both, to withdraw the consent or exercise rights under the act or make a complaint to the board.	• Notice must be clear and easily accessible, without hiding important details in separate terms and conditions or redirecting to unclear FAQs. This ensures that the Data Principal has all the required information at one place for informed decision-making on consent. • The management should create a concise itemised list of personal data. • In some cases, businesses might deliver notices in a paper format. The draft rules do not specify what must be included in such notices, where adding a website or app link is not possible.
Chapter II Section 6 - Consent, Clause 7 and 8	The Data Principal can give, manage, review or withdraw their consent through a Consent Manager. The Consent Manager will be accountable to the Data Principal and shall act on their behalf.	**Rule 4** Prerequisite for Consent Manager companies: • incorporated in India • minimum net worth of INR 2 crore • interoperable platforms for consent management • reputation for fairness and integrity • appropriate technical and organisational measures • no conflict of interest with the registered Data Fiduciaries • adhere to the defined obligations such as: - maintaining the website or app through which Data Principals access services/consents - keep records of consents, accompanying notices and personal data shared with transferee Data Fiduciaries for at least 7 years.	• Any entity with the necessary infrastructure to act as a consent manager should use it only for internal purposes without a conflict of interest with the data fiduciary. So, if an entity can maintain this integrity, they can offer their platform to other firms to explore business opportunities. • Consent manager should store records for at least seven years or longer as agreed upon by the data principal, or as required by the law. But for a few industries, data should be deleted within three years. So, consent managers must have built-in capabilities to meet these data retention requirements.

Our perspective on key tenets

Reference to the act	Requirement in the act	Proposed rules	Our perspective
Chapter II, Section 7 - Certain Legitimate uses, Clause 7 (b)	The State and its instrumentalities may process personal data to provide subsidy, benefit, service, certificate, licence or permit as prescribed, where: • the Data Principal has previously consented to the processing of their personal data • personal data is available in a digital form, or in a non-digital form which is subsequently digitised from any database, register, book or other document maintained by the state and its instrumentalities.	**Rule 5** The State and its instrumentalities may process the personal data under certain legitimate uses such as providing subsidies, benefits, services, certificates, licences and permits and will have to adhere to certain technical and organisational measures while processing such data.	• The draft rules clarify how the State and its instrumentalities should process personal data for legitimate use, while intimating the contact information of the person who is answerable to the data principal about processing personal data, specifying communication link to access the website or the app.
Chapter II, Section 8 - General obligations of data fiduciary, Clause 5	A Data Fiduciary shall protect personal data in its possession, or under its control, including data processed on its behalf by a data processor, by taking reasonable security safeguards to prevent data breach.	**Rule 6** A Data Fiduciary shall protect personal data in its possession or under its control by taking reasonable security measures, such as: • encryption, obfuscation, masking or use of virtual tokens • access control to computer resources • visibility on data accessed through logs, thereby enabling detection, investigation and remediation of unauthorised access • regular backup of data ensuring continuity in case of compromise, destruction or loss of access • retain logs for one year, unless required otherwise by the law • having appropriate contractual obligations on the data processor for reasonable security safeguards • implementing technical and organisational measures.	• The draft rules list the privacy and security techniques to be implemented, with room for Data Fiduciaries to upgrade their privacy and security infrastructure. • Maintaining the audit trail for a year will assist fiduciaries to demonstrate compliance and take reasonable actions during any incident. • Implementing these controls may increase operational costs for the Data Fiduciary, which can be a challenge for small organisations. • Maintaining an efficient data backup mechanism will require a robust business continuity program (BCP). • The draft rules do not outline the accountability and contractual obligations of the data processor for maintaining reasonable security measures. • The draft rules do not clarify if the security measures apply to all Data Fiduciaries irrespective of their size and scale.

Our perspective on key tenets

Reference to the act	Requirement in the act	Proposed rules	Our perspective
Chapter II, Section 8 - General obligations of data fiduciary, Clause 6	The notification of personal data breach shall be given by the Data Fiduciary to: • the board • affected Data Principals.	**Rule 7** Data Fiduciary shall notify the breach to: • the board – within 72 hours of becoming aware or a longer period – as permitted by the board • affected Data Principals in a concise, clear and plain manner, without delay through user account or any mode of communication registered by them. The notification shall include: • a description of the breach • consequences of the breach • measures implemented to mitigate risk • safety measures that data principal may take to protect themselves • business contact information of a representative • facts related to the event, reasons leading to the breach and any findings regarding the person who caused the breach.	• The draft rule for the personal data breach notification is detailed and comprehensible. Data fiduciaries shall update, or document new policy/procedure aligned with the act and draft rules to ensure compliance. • In case of a data breach, the draft rules do not provide a mechanism to notify the Data Protection Board or specify if they must inform guardians or parents of children or persons with disabilities about the incident. • The draft rules do not mandate a time period for communicating about the breach to the data principal, which is practical, as each breach needs to be investigated before notification.
Chapter II, Section 8 - General obligations of data fiduciary, Clause 7 and 8	The Data Fiduciary shall erase the personal data when: • either Data Principals withdraw their consent • or the intended purpose is fulfilled – whichever is earlier • or if required by the law. A Data Fiduciary shall obligate its data processor to erase the personal data as per the defined period, or as communicated. The data principal can request the Data Fiduciary to exercise their rights for a specific time period. This may vary depending on the class of the Data Fiduciaries and purposes.	**Rule 8** E-commerce entities (with >2 crore users in India), gaming intermediaries (with >50 lakhs users in India) and social media intermediaries (with >2 crore users in India) must erase personal data after three years from the date the Data Principal last approached the fiduciary, except for enabling the Data Principal to access their account or any virtual tokens issued by or on behalf of the Data Fiduciary Intimate the Data Principal at least 48 hours before deletion of their data unless they login to their account or initiate contact with the Data Fiduciary.	• As per Consumer Protection Act 2019, ‘e-commerce’ means buying or selling of goods or services, including digital products, over digital or electronic network. Hence, all organisations with an online presence (website and/or app) for accepting and delivering goods and services come under the purview of this rule. • This compliance may reduce storage costs but could impact marketing and analytics. It may also require updates to data management systems for proper identification and deletion of personal data.

Our perspective on key tenets

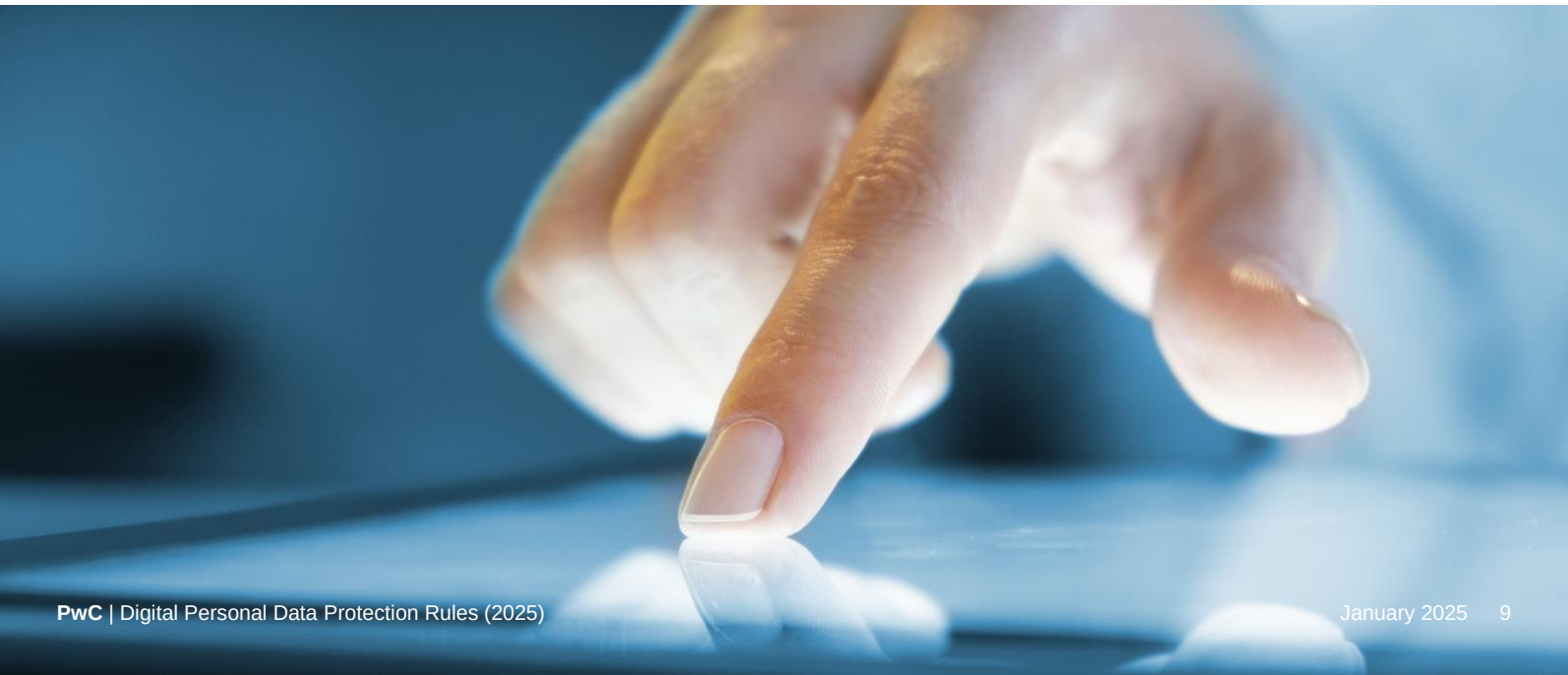
Reference to the act	Requirement in the act	Proposed rules	Our perspective
Chapter II, Section 8 - General obligations of data fiduciary, Clause 9	Data Fiduciary shall publish the business contact information of a DPO or a person who is able to answer the queries of the Data Principal about the processing of their personal data on behalf of the Data Fiduciary.	**Rule 9** Data Fiduciary shall publish their business contact or their DPO on the website or the app. The fiduciary must also share these contacts in every communication with the Data Principal with regard to exercising their DPDP rights.	• The draft rules re-emphasise that the contact person or DPO appointee should be accessible for data principals on websites, mobile apps and other relevant communication platforms.
Chapter II, Section 9 - Processing of personal data of children	The Data Fiduciary shall: • obtain verifiable consent from the parent or lawful guardian before processing the personal data of a child or a person with disability who has a lawful guardian • refrain from processing any personal data that is likely to cause any detrimental effect on the well-being of a child • refrain from tracking, behavioural monitoring and targeted advertising directed at children. The above-mentioned provisions shall not be applicable to the processing of the personal data of a child by the classes of Data Fiduciaries or for such purposes, and subject to such conditions, as may be prescribed.	**Rule 10** A Data Fiduciary shall adopt appropriate technical and organisational measures to ensure that verifiable consent of the parent is obtained before processing any personal data of a child and from individuals identifying themselves as the lawful guardian of a person with disability. Fiduciary must ensure that the individual identifying as the parent is an adult and is identifiable through: • reliable details of identity and age available with the Data Fiduciary • voluntarily provided details of identity and age • a virtual token mapped to the same • the guardian is appointed by a court of law, a designated authority or a local level committee, under the law applicable to guardianship. Exceptions apply to Data Fiduciary classes such as educational institutions, clinical establishments, mental health establishments and healthcare professionals – subject to not undertake tracking or behavioural monitoring or targeted advertising for children.	• The Data Fiduciary will require technological and process changes to obtain verifiable consent from parents or guardians. This poses challenges to verify the age and identity of the individual identifying as the parent, and integrating systems with external entities entrusted by law or the Central Government (UIDAI, DigiLocker, etc.).

Our perspective on key tenets

Reference to the act	Requirement in the act	Proposed rules	Our perspective
Chapter II, Section 10 - Additional obligations of SDF	The SDF shall: • appoint a DPO • appoint an independent data auditor • undertake the periodic DPIA • conduct periodic audits • implement other measures consistent with the provisions of the act, as may be prescribed.	**Rule 12** SDF shall: • undertake DPIA and data privacy audits once a year • furnish the report to the board containing significant observations in the DPIA and audit • observe due diligence to verify that algorithmic software deployed are not posing a risk to the rights of Data Principals • ensure that personal data specified by the central government is processed subject to the restriction that the personal and traffic data pertaining to its flow is not transferred outside India.	• The draft rules clarify the additional obligations of SDFs, and they must make additional efforts to ensure compliance. • The criteria for classification of SDFs is unclear. • While the draft rules do not clarify what algorithmic software is, SDFs using personal data for the purpose of training models need to reconsider their processes, in case a Data Principal withdraws consent. • The draft rules do not clarify how and when the central government will define the personal data that must be processed within India's borders. Additionally, these draft rules reinforce data localisation requirements across all industry sectors, which were originally applicable only to payment system providers under a Reserve Bank of India (RBI) regulation.
Chapter III Section 11 - 14- Rights of Data Principal	The Data Principal has the following rights: • right to access information about personal data • right to correction and erasure of personal data • right of grievance redressal • right to nominate.	**Rule 13** The Data Fiduciary and Consent Manager (as applicable) shall publish on their website or app or both: • how a Data Principal can raise a request • the particulars of the identifier of a Data Principal, which may be required to identify them (as applicable) • the period of response under its grievance redressal system. The Data Principal has the right to nominate one or more individuals to act on their behalf under the right to nominate.	• These rights reflect the act's central theme, which is to empower individuals to control their information and how organisations collect, process and share it. Data Fiduciaries and Consent Managers must develop processes and technology solutions to address Data Principals' rights requests. • The draft rules do not define the maximum time allowed for Data Fiduciaries and Consent Managers to address grievances. Without a specified timeframe for grievance redressal, the rights granted to data principals under the DPDP Act may be weakened.

Our perspective on key tenets

Reference to the act	Requirement in the act	Proposed rules	Our perspective
Chapter IV, Section 16 - Processing of personal data outside India, Clause 1 and 2	The central government may impose restrictions on the transfer of personal data by a Data Fiduciary to any country or territory outside India. This does not impact any existing laws in India that provide protection or restrictions on transferring personal data by a Data Fiduciary outside India.	**Rule 14** The transfer of personal data processed by a Data Fiduciary to any country or territory outside India is subject to the condition that the Data Fiduciary must comply with the requirements set by the central government. These requirements may be specified through general or special orders.	• The current draft rule will have an annexure with more details regarding the transfer of data outside India. • If the processing of personal data by Data Fiduciaries outside India is restricted by a future government order, organisations that use cloud services or process personal data abroad will need to reconsider their IT strategy and architecture to maintain compliance with the DPDP Act 2023.
Chapter IV, Section 17 - Exemptions, Clause 2	The act does not apply when: • the central government may notify, in the interests of sovereignty and integrity of India, security of the state, friendly relations with foreign states, maintenance of public order or preventing incitement to any cognisable offence relating to any of these. • data is necessary for research, archiving or statistical purposes, as long as it is not going to be used to take any decisions specific to a Data Principal and such processing is carried out in accordance with such standards as may be prescribed.	**Rule 15** The provisions of the act shall not apply to the processing of personal data necessary for research, archiving or statistical purposes if it is carried out in accordance with the standards specified in the second schedule.	• The definitions of ‘research’, ‘archival’ and ‘statistical purpose’ are not clearly defined in the draft rules. For instance, it is not clear whether clinical trials and medical device research fall under the category of ‘research’ under the act.



02

Key responsibilities

Key responsibilities of a data fiduciary

Data privacy notice

Presented in an understandable and clear language

- Description of personal data
- Purpose of processing
- Description of the goods or services to be provided
- Description of means using which the data principal may withdraw his/her consent, exercise their rights and make a complaint to the board

Personal data security

Protect the personal data including any processing undertaken by the Data Fiduciary or on its behalf by a data processor.

- Securing of personal data through encryption, obfuscation, masking or the use of virtual tokens mapped to the personal data
- Access control for the computer resource used
- Maintaining, monitoring and reviewing logs
- Retaining logs and personal data for detection, investigation, remediation and continuous processing for one year
- Data backups and any other means for continued processing
- Appropriate contractual clauses between Data Fiduciary and data processor for undertaking reasonable security safeguards
- Appropriate technical and organisational measures

Key responsibilities of a data fiduciary

Notification of personal data breach

Send notifications to each affected Data Principal in a concise, clear manner and without delay, and to the board within 72 hours of becoming aware – or within a longer specified period as allowed by the board.

- Description of the breach, including its nature, extent and the timing and location of its occurrence
- Consequences that are likely to arise from the breach
- Measures implemented and being implemented to mitigate risk
- Safety measures that the Data Principals may take to protect their interests
- Business contact information of a representative
- Any findings regarding the person who caused the breach
- A report regarding the intimations given to affected data principals

Personal data deletion

- Inform the Data Principal at least 48 hours before completion of the time period for erasure.
- Intimate the Data Principal about the deletion unless they log into their user account or initiate contact with the fiduciary for the specified purpose of data privacy rights.

Publishing the contact information

- Publish the business contact information of the DPO or a representative.
- Publish the details on the website or app, and in every response to a communication for the exercise of the rights.

Verifiable consent from parents and/or guardians

- Adopt necessary technical and organisational measures to ensure that verifiable consent is obtained from the parent before processing the child's personal data and to verify that the guardian is appointed by a court of law or a designated authority under appropriate law.
- Such parent or guardian shall be adult and shall be identifiable as required by the following references:
  - reliable details of identity and age available with the fiduciary
  - voluntarily provided details of identity and age
  - virtual token mapped to the details of the parent
  - token verified and made available by a digital locker service provider.

Data privacy rights

- Publish the means using which a Data Principal can make a request on the website or app.
- Additionally publish:
  - the particulars or identifier number* which is required to identify the Data Principal
  - the period for grievance redressal and for responding to the grievances.

***Identifier** means any sequence of characters issued by the Data Fiduciary to identify the Data Principal and includes a customer identification file number, customer acquisition form number, application reference number, enrolment ID or licence number that enables such identification.

Key responsibilities of a data fiduciary

Performing DPIAs and audits for SDFs

- Perform periodic DPIAs and data privacy audits.
- Perform a DPIA once every 12 months from the date on which they were notified as an SDF.
- Conduct an audit once every 12 months to ensure effective observance of the act and draft rules.
- Furnish significant observations from the DPIA and audit to the board.

Risk assessment for SDFs

- Observe due diligence to verify that algorithmic software deployed for hosting, display, uploading, modification, publishing, transmission, storage, updating or sharing of personal data processed are not likely to pose a risk to the rights of Data Principals.

Cross-border data transfer for SDFs

- Align cross-border data transfer with the central government's notification.
- Undertake measures to ensure that personal data and traffic data, specified by the central government through a future general or special order, is not transferred outside the territory of India.

Personal data deletion

- Erase personal data, unless its retention is necessary for compliance with any law.
- Intimate the Data Principal about the deletion unless he/she logs into their user account** or initiates contact with the Data Fiduciary for a specified purpose or exercise their data privacy rights.

** **User account** means the online account registered by the Data Principal with the Data Fiduciary and includes any profiles, pages, handles, email addresses, mobile numbers and other similar presences by means of which she is able to access the services of such Data Fiduciary.

Time period for deletion of data by SDFs

Sr. no.	Class of data fiduciaries	Purposes	Time period
1	A Data Fiduciary who is an e-commerce entity with at least 2 crore registered users in India	For all purposes, except for the following: a) enabling the Data Principal to access their user account; and b) enabling the Data Principal to access any virtual token that is issued by or on behalf of the Data Fiduciary, is stored on the digital facility or platform of such Data Fiduciary, and may be used to get money, goods or services.	Three years from the date on which the Data Principal last approached the Data Fiduciary for the performance of the specified purpose or exercise of their rights, or the commencement of the Digital Personal Data Protection Rules, 2025, whichever is latest
2	A Data Fiduciary who is an online gaming intermediary with at least 50 lakh registered users in India		
3	A data fiduciary who is a social media intermediary with at least two crore registered users in India		

E-commerce entity

Any person who owns, operates or manages a digital facility or platform for e-commerce as defined in the Consumer Protection Act, 2019 (35 of 2019), but does not include a seller offering her goods or services for sale on a marketplace e-commerce entity as defined in the said act.

As per Consumer Protection Act, 2019, 'e-commerce' means buying or selling goods or services including digital products over digital or electronic networks.

Online gaming intermediary

Any intermediary that enables the users of its computer resource to access one or more online games.

Social media intermediary

An intermediary as defined in the Information Technology Act, 2000 (21 of 2000) who primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using her services.

Key responsibilities of consent managers

Conditions for the registration of a consent manager

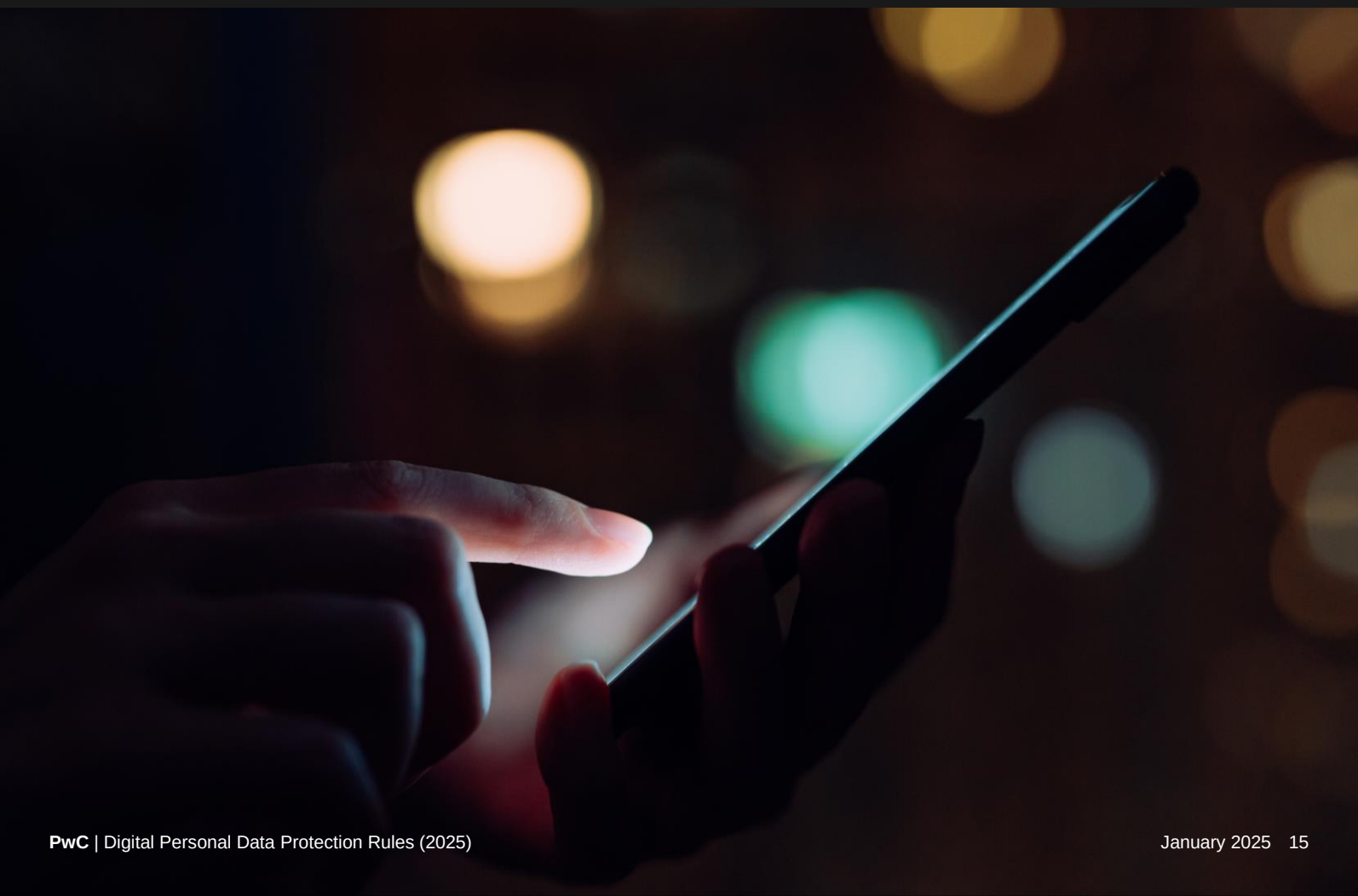
- Company incorporated in India
- Has sufficient capacity, including technical, operational and financial capacity, to fulfil the obligations
- Financial condition and the general character of management are sound.
- Net worth of the applicant is not less than INR 2 crore
- Volume of business that is likely to be available and adequate capital structure and earning prospects
- The directors, key managerial personnel and senior management are individuals with a general reputation and record of fairness and integrity.
- The memorandum of association and articles of association contain no conflict of interest with the fiduciary and its key stake owners and have measures to ensure the same.
- The proposed operations are in the interest of the Data Principals.
- It is independently certified that:
    a) the platform for Data Principals is interoperable
    b) appropriate technical and organisational measures have been implemented.

Obligations of a consent manager

- Enable a Data Principal to give consent for the processing of personal data by a Data Fiduciary using its platform, directly or through another Data Fiduciary onboarded onto the platform.
- Ensure that the manner of making available the personal data or its sharing is such that the contents are not readable by it.
- Maintain on the platform a record of:
    a) consents given, denied or withdrawn
    b) notices preceding or accompanying requests for consent
    c) sharing of personal data with a transferee Data Fiduciary.
- The consent manager shall:
    a) give access to the record-using platform
    b) make the Data Principal's information available in a machine-readable form on request
    c) maintain a record for at least seven years or for a longer period, as agreed between the Data Principal and Consent Manager or as required by law.
- Develop and maintain a website or app or both as the primary means through which a Data Principal may access the services provided by the Consent Manager.
- The Consent Manager shall not sub-contract or assign the performance of any of its obligations.
- The Consent Manager shall take reasonable security safeguards to prevent any personal data breach.
- The Consent Manager shall act in a fiduciary capacity in relation to the Data Principal.
- The Consent Manager shall avoid a conflict of interest with Data Fiduciaries, including their promoters and key managerial personnel.
- The Consent Manager shall have measures to ensure that no conflict of interest arises on account of its directors, key managerial personnel and senior management holding a directorship, financial interest, employment or beneficial ownership in Data Fiduciaries or having a material pecuniary relationship with them.
- The Consent Manager shall publish information regarding:
    a) the promoters, directors, key managerial personnel and senior management of the company
    b) individuals who hold more than 2% of the shareholding
    c) every corporate whose shares (more than 2%) are held by the promoter, director, key managerial personnel or senior management
    d) any other information as directed by the board
- The Consent Manager shall have in place effective audit mechanisms to review, monitor, evaluate and report the outcome of such audit to the board periodically and on such other occasions as the board may direct.
- The control of the company registered as the Consent Manager shall not be transferred by way of sale, merger or otherwise, except with the previous approval of the board and subject to fulfilment of conditions as specified by the board.

Key responsibilities of the state

- Process data for a specified purposes to provide or issue to the Data Principal subsidy, benefit, service, certificate, licence or permit, or for the performance of any judicial or quasi-judicial or regulatory or supervisory function.
- Implement appropriate technical and organisational measures.
- Collect and process only the data necessary to achieve a specific purpose.
- Retain personal data till required or for compliance with any law for the time being in force.
- Implement reasonable security safeguards to prevent personal data breaches.
- Identify accountability of the person who alone or in conjunction with other persons determines the purpose and means of processing the personal data.
- When processing personal data to provide or issue to the data principal subsidy, benefit, service, certificate, licence or permit:
  - provide business contact information of a person who is able to answer all data privacy queries.
  - specifying the particular communication link for accessing the website or app, or both.
  - provide a description of means for exercising the data privacy rights.
  - carry out processing in a manner consistent with such other standards as may be applicable.



About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 151 countries with over 360,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

Contact us

Sivarama Krishnan

Partner and Leader – Risk Consulting, PwC India
sivarama.krishnan@pwc.com

Anirban Sengupta

Partner and Leader – Business and Technology Risk, PwC India
anirban.sengupta@pwc.com

Heena Vazirani

Partner – Business and Technology Risk, PwC India
heena.vazirani@pwc.com

S Dinesh

Partner – Business and Technology Risk, PwC India
s.dinesh@pwc.com

Contributors

Heena Vazirani

Faizan Sarwar

Amey Tipnis

Krishna Veni Pandelapalli

Vaishnavi Shukla

Rodney Dsouza

Editorial

Rashi Gupta

Design

G Gnanaraj

Data Classification: DC0 (Public)

GG/January 2025-M&C 43275