



Draft DPDP Rules 2025: Guidance to DPDP act implementation



January 2025

[kpmg.com/in](https://www.kpmg.com/in)

KPMG. Make the Difference.



Target Areas for DPDP Rules 2025

The Digital Personal Data Protection Rules, 2025* released by the Ministry of Electronics and Information Technology, India (MeITY) on 3 January 2025 serves as a crucial extension to the Digital Personal Data Protection Act 2023, providing operational clarity that complement the foundational principles of the act. By outlining specific compliance requirements, these rules facilitate a smoother transition for businesses aiming to align with the act. These rules act as a stepping-stone by offering directives on data protection practices, thereby enabling businesses to implement robust data governance framework which would not only ensure legal compliance but also foster trust and transparency with data principals, ultimately contributing to a more secure and privacy-conscious business environment.



* Please note that Digital Personal Data Protection Rules 2025 are draft Rules released by the MeITY for public consultation.




Below are the Target Areas for DPDP Rules 2025

01		Intimation of personal data breach	5
02		Notice, consent overview and verifiable consent	5
03		Obligations of consent manager	6
04		Reasonable security safeguards	7
05		Empowering data principals	7
06		Cross border data transfer	8
07		Retention period	8
08		Obligations of significant data fiduciary	9
09		Exemptions	9

Key timelines in the rules

DPDP Rules	Obligation	Timeline(s)
7(1) and 7(2)	Breach intimation to the Data Protection Board (DPB)	First Intimation: Without delay Second Intimation: Within 72 hours
8(2) -Third Schedule	Personal data erasure and intimation of such erasure by Ecommerce/social media/gaming entities	Retention Period: Three years Intimation: 48 hours prior to deletion
12(1)	Periodicity of DPIA and Data Audit	Yearly from: <ul style="list-style-type: none"> • Rules coming into force (or) • Fiduciary becomes SDF.
First Schedule – Part B - 4(c)	Maintenance of consent records by consent manager	Seven years

Publishing contact details





-  Data fiduciary (DPO, in case of SDF) should publish business contact details of designated person on its website or application
-  Data fiduciary should mention the contact information of designated person (DPO, in case of SDF) in every response to the communication from data principal exercising their rights
-  Designated person should be able to answer questions about personal data processing on behalf of the data fiduciary.



1. Intimation of personal data breach

1. Primary intimation (to DPB)	<p>To be intimated without delay upon becoming aware of the breach.</p> <p>Details to be included:</p> <p>Description of the breach including nature, extent, likely impact, timing, location of the occurrence</p>	3. Intimation to data principal
2. Secondary intimation (to DPB)	<p>To be intimated within 72 hours upon becoming aware or a longer period approved by DPB.</p> <p>Details to be included:</p> <ul style="list-style-type: none"> Updated information from first intimation Broad facts relating to events, circumstances and cause of breach Implemented or proposed measures to mitigate risk Findings regarding person who caused the breach Remedial measures taken to prevent recurrence Report of notification to data principals. 	<p>Data principals should be intimated without delay, to the best of its knowledge upon becoming aware of the personal data breach:</p> <p>Details to be included:</p> <ul style="list-style-type: none"> Description of the breach (nature, extent, timing and location) Measures implemented or being implanted for mitigation Safety measures to protect their interest Contact information of person who can respond for Data fiduciary. <p>Mode of communication:</p> <ul style="list-style-type: none"> User account (includes any profiles, pages, handles, email address, mobile number and other similar means); or Any mode registered with the data fiduciary.

2. Privacy notice

 <p>Independent information</p>	<p>Notice needs to be understandable without any other information that is made available by the data fiduciary</p>
 <p>Format</p>	<p>Provides a fair account of details necessary, in clear and plain language for providing specific and informed consent</p>
 <p>Minimum contents</p>	<p>A notice, at a minimum should contain:</p> <ul style="list-style-type: none"> Itemised description of personal data Details of the specific purpose and provide an itemised description of the goods or services to be provided or the uses to be enabled by such processing.
 <p>Means of communication</p>	<p>Data fiduciaries need to provide a link to a website or application or both and description of other means which enables a data principal to:</p> <ul style="list-style-type: none"> Withdraw their consent* Exercise their data principal rights Make a complaint to the Board.

***Note:** The ease through which consent can be withdrawn should be comparable to the ease through which consent is collected.

Consent overview



Consent manager
registration



Consent manager
obligations



Verifiable
consent

Verifiable Consent

Ensure verifiable consent is obtained from parent/guardian for processing personal data of a child or a person with disability

Ensure appointment of guardian is valid and such guardianship extends to the consent provided

Data fiduciary must verify that the parent/guardian is an adult by using reliable identity details or through a virtual token mapped to such details.

Consent needs to be reliable if identification is required in certain cases



Who can register as consent manager?



Company incorporated in India



Net worth > INR2 Crores



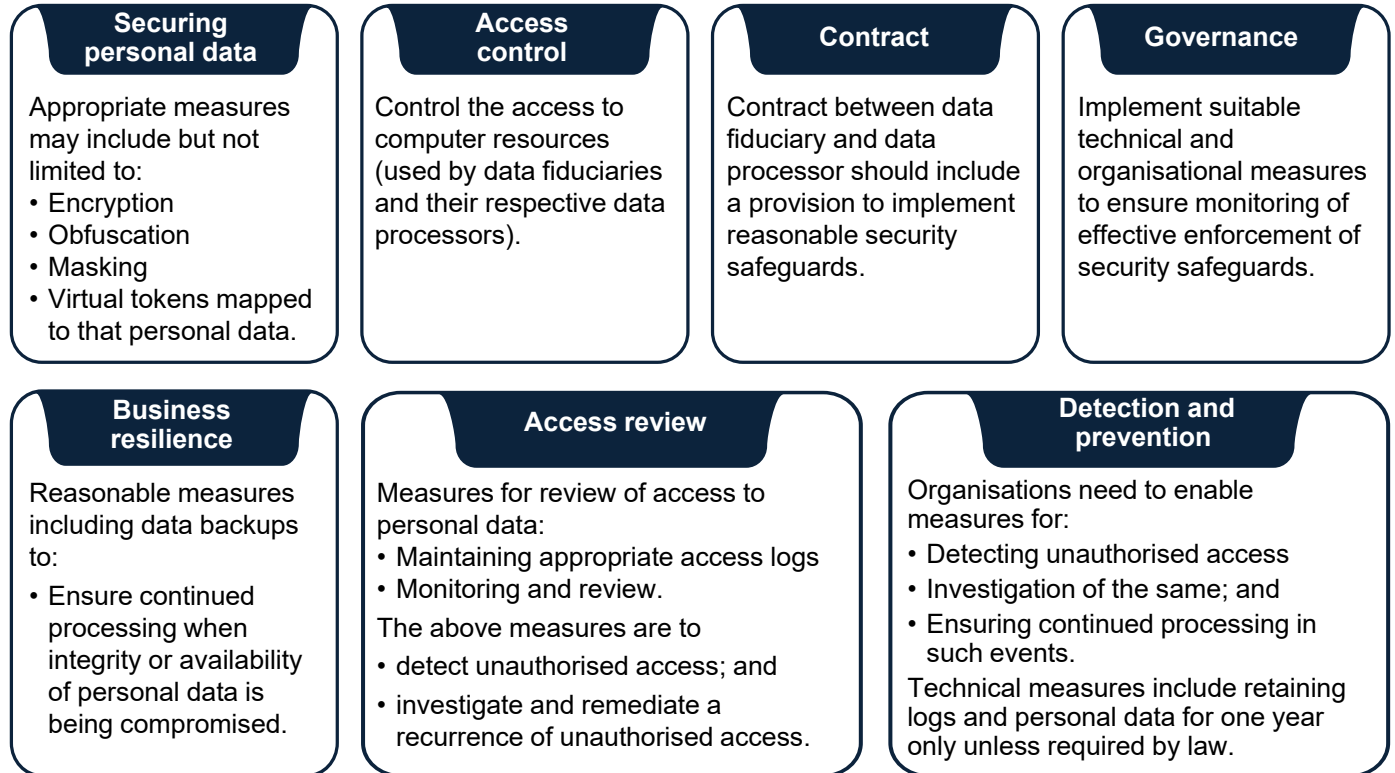
Technical, operational and financial capacity

3. Obligations of consent manager


- Services need to be primarily provided through an application/website
- Disclosures about certain company information on the application/website
- Implement reasonable security safeguards to prevent data breach
- Ensure personal data access or sharing is done in a manner where the contents are not readable
- Prohibit sub-contracting or assigning performance of any of its obligations
- Avoid conflict of interest with data fiduciaries and take measures for the same
- Independent certification for the interoperable platform
- Consent management platform digitally accessible by data subject to manage, review and withdraw their consent
- Retain data principal records for seven years or longer if agreed with data principal or as required by law
- Establish effective audit mechanism to periodically report the outcomes to the Board.

4. Reasonable security safeguards

Organisations also need to ensure effective observance of the below security safeguards



5. Empowering Data Principals




Data fiduciary and consent managers' role

Clearly publish on their website or application (or both):

- The process by which data principals can exercise their rights, including particulars such as usernames or identifiers*
- Provide clear timelines for responding to grievances of the data principals and implement appropriate technical and organisational measures under their grievance redressal system.

*Note: identifier here, refers to 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 license number that enables such identification.





Data principal's role

- To exercise her rights under the act, the data principal can request to access and erase their personal data by contacting the data fiduciary
- Data principals may nominate one or more individuals to exercise their rights under the DPDP act, in accordance with the terms of service of the fiduciary and any applicable law using the data fiduciary's mechanism.




6. Cross border data transfer

Transfers outside India by data fiduciaries are subject to requirements set by the central government for making personal data available to any foreign state

7. Retention period as per third schedule

 <p>Erasure of personal data</p> <p>Data fiduciary must erase personal data if data principal does not approach –</p> <ul style="list-style-type: none"> • For specified time period or; • Exercise rights within the specified time mentioned in third schedule of the rules. 	 <p>Notification before erasure</p> <ul style="list-style-type: none"> • Data fiduciary must inform the data principal at least 48 hours before the erasure of personal data • Upon completion of aforementioned period, data fiduciary shall erase the data unless data principal logs into their user account or contact the data fiduciary to prevent erasure.
--	---

Erasure and retention period for certain data fiduciaries

Class of data fiduciaries	Purpose	Time period
 <p>E-commerce entity with not less than two crore registered users in India</p>	<p>All purposes except -</p> <ul style="list-style-type: none"> • Access to user account • Access to virtual tokens for money, goods or services. 	<p>Three years from the date Data Principal last approached for the performance of the specified purpose or exercise of their rights or commencement of the Rules, whichever is earlier.</p>
 <p>Online gaming intermediary with not less than 50 lakhs registered users in India</p>	<p>All purposes except -</p> <ul style="list-style-type: none"> • Access to user account • Access to virtual tokens for money, goods or services. 	<p>Three years from the date Data Principal last approached for the performance of the specified purpose or exercise of their rights or commencement of the Rules, whichever is earlier.</p>
 <p>Social Media Intermediary with not less than two crore registered users in India</p>	<p>All purposes except -</p> <ul style="list-style-type: none"> • Access to user account • Access to virtual tokens for money, goods or services. 	<p>Three years from the date Data Principal last approached for the performance of the specified purpose or exercise of their rights or commencement of the Rules, whichever is earlier.</p>

8. Obligations of significant data fiduciary



Observe due diligence to verify that any algorithmic software for processing personal data are not likely pose a risk to the rights of data principals.

Data Protection Impact Assessment and Periodic Audit shall be conducted once every 12 months and results should be furnished to the Board by the person carrying out the same.

Adopt measures to ensure personal data and its related traffic data identified by the Central Government are processed in compliance with specific restrictions and not transferred outside of India.

9. Exemptions

Exemptions are available with conditions from processing personal data of children for:

- Clinical establishments
- Mental health establishments or healthcare professionals,
- Allied healthcare professionals
- Educational institutions
- Individuals (fiduciary) to whose care infants and children in a crèche or child day care centers are entrusted
- Fiduciaries engaged by an educational institution, crèche or child care center for transport of children enrolled with such institution, crèche or center.

Exemption from research, archiving and statistical purposes if processing is carried on in accordance with these standards:

- Processing is for certain exemptions under the act
- Processing personal data only to the extent necessary for the purposes
- Implementing mechanisms to ensure personal data accuracy
- Retention of personal data to the extent it is necessary
- Implement reasonable security safeguards for preventing personal data breaches
- Processing is for the state and any of its instrumentalities to provide or issue to the data principal such subsidy, benefit, service, certificate, license or permit. During such processing, the same is undertaken while providing intimation to data principal
- Ensuring accountability of person(s) determining the means and purposes of processing to comply with the above standards.

Exemptions available from processing of the personal data of children for:

- Performance of any function or discharge of any duties in the interests of a child under law
- Providing or issuing of any subsidy, benefit, service, certificate, licence or permit, by whatever name called, under law or policy or using public funds, in the interests of a child
- Creation of a user account for communicating by email
- Ensuring that information likely to cause any detrimental effect on the well being of a child is not accessible to her
- Data fiduciary to confirm that the data principal is not a child and observance of due diligence of verifiable consent.

KPMG in India has got you covered . . .

The privacy compliance landscape is undergoing a substantial transformation with draft Digital Personal Data Protection Rules, 2025.

This landmark legislation is set to introduce a comprehensive and rigorous framework for data protection, fundamentally changing how the industry manages consumer information. Companies will be required to overhaul their data management practices to ensure enhanced security and transparency.

Companies must implement advanced data governance measures including robust data protection strategies and adhere to principles such as data minimisation and secure processing. They will also need to facilitate data subject rights related to data access, correction etc. By adhering to these, organisations are set to bolster consumer trust and ensuring more rigorous stewardship of personal data.

KPMG in India’s privacy portfolio boasts a variety of services that can help businesses manage regulatory obligations and leverage data to create value and increase revenue while meeting the expectations of customers, employees and vendors. With KPMG in India’s extensive privacy and data protection experience, businesses can evolve and develop a tailored, structured and flexible approach – helping unlock economic potential while also helping to ensure data privacy.



KPMG in India’s data privacy offerings

Privacy regulatory landscape assessment:
Determine your regulatory obligations and assess the current privacy risk posture

Privacy strategy and operations governance:
Design and advise on the implementation of privacy program, governance accountability model, and building privacy first culture.

Personal data protection:
Obtain visibility over personal data and establish controls to secure the personal data lifecycle.

Privacy by design:
Build privacy-enhancing technology stack and digital approaches to manage regulatory expectations.

Third-party privacy risk management:
Governance over personal data sharing with third parties to manage data privacy risks.

Privacy training program and e-learning:
Create targeted awareness at the enterprise level.

Privacy managed services:
Provide ongoing support to run privacy and data protection office and assist you in managing your strategic and operational data privacy control environment.

Platform approach to privacy:
Internalise privacy program by automating privacy operations and establishing governance over personal data use across the enterprise.

KPMG in India can offer a global, multidisciplinary view of risk, helping you address your privacy challenges. KPMG in India is committed to offer precision, quality and objectivity, which can help you embed protection and trust into your activities, not just your technology, to create a security and privacy culture for an organisation.

Acknowledgements

We are extremely grateful to subject matter experts, and KPMG in India team members for extending their knowledge and insights to develop this document.

Authors

- Amrita
- Ayushi Dasgupta
- Mala Lahoti
- Shubhankar Mathur
- Tanishka Prasad
- Aswinisri Narayanan
- Shubhra Murali

Design and compliance

- Karthika Prabasankar
- Nidhi Agarwal

KPMG in India contacts:

Akhilesh Tuteja
Global Head – Cyber Security
E: atuteja@kpmg.com

Atul Gupta
Partner, HoF - Digital Trust
E: atulgupta@kpmg.com

Nitin Shah
Partner, Digital Trust
Head, Cyber and Privacy
Strategy and Governance
E: nitinshah@kpmg.com

Shikha Kamboj
Partner, Digital Trust
National Lead,
Data Privacy and Ethics
E: skamboj@kpmg.com

Kanika Jain
Associate Partner, Digital Trust
Data Privacy and Ethics
E: kanikajain@kpmg.com

Vipul Ubale
Associate Partner, Digital Trust
Data Privacy and Ethics
E: vipulubale@kpmg.com

Rupak Nagarajan
Director, Digital Trust
Data Privacy and Ethics
E: rupak@kpmg.com

Nakuleesh Sharma
Director, Digital Trust
Data Privacy and Ethics
E: nakuleesh@kpmg.com

Amrita
Director, Digital Trust
Data Privacy and Ethics
E: amritakumar@kpmg.com

kpmg.com/in



Access our latest insights
on KPMG Insights Edge

Follow us on:

kpmg.com/in/socialmedia



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011
Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2025 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.

This document is for e-communication only (022_THL1224_KP)