protiviti®
Global Business Consulting

DATA PRIVACY IN DIGITAL INDIA

DECONSTRUCTING THE DRAFT DPDP RULES, 2025

Face the Future with Confidence®

TABLE OF CONTENTS

INTRODUCTION

The Digital Personal Data Protection Act, 2023 marked a transformative moment for India's data protection landscape, establishing a robust framework for privacy governance, clear compliance obligations, and well-defined rights for individuals. Taking a pivotal step forward, the Ministry of Electronics and Information Technology (MeitY) grabbed the attention of 1.43 billion people in India and the global regulators on January 3, 2025, by unveiling the draft DPDP rules for public consultation, marking a significant moment in India's data protection journey.

The Act focused primarily on digital personal data of Indian residents and aimed to provide them with greater transparency and control on how their personal data is being used. The act in line with other global data protection regulation talks notice requirements, consent, and rights of data principals. In addition, it also outlined the obligations of data fiduciaries, data principal and data processors, and penalties in case of non-compliance for both the fiduciary and the principal. Now, in 2025, the draft DPDP rules has provided us the next step of the evolving privacy framework, which further list down the operational elements and compliance requirements for the data protection regulation in India. The Act broadly outlined the 'what' and 'why' of data privacy, the draft rules now serve as an enabler, addressing the 'how'—providing much- needed clarity on compliance measures for Data Fiduciaries and the privacy expectations of Data Principals.

Building on the legislative advancements, businesses in India are presented with valuable opportunities to enhance their operations and compliance efforts as they work towards fully implementing the provisions of the Act. We observed during 1 CII-Protiviti State of Data Privacy in India 2024 survey, conducted in collaboration with CII (Confederation of Indian Industry), 63% of organizations highlighted that inconsistent implementation remains a major challenge, while they already have a privacy policy in place.

Additionally, organizations expressed concerns regarding cross-border data transfers, data breaches, and the lack of sector-specific clarity in the Act.

This paper will focus on how the recently released rules have addressed several concerns of the organizations which were also highlighted in the CII-Protiviti State of Data Privacy In India Survey Report, 2024. Let's delve into the details of the Rules, examining what has been made clear and what still requires further clarity, helping organizations navigate this evolving regulatory landscape with confidence.

Source

1 https://www.protiviti.com/in-en/state-of-data-privacy-in-india-survey-report-2024

KEY TENANTS OF
DRAFT DPDP RULES, 2025

With the release of the draft DPDP rules, organizations will now have better clarity on how to implement the guidelines to ensure compliance with the regulation. These rules help in providing clear direction on some of the key aspects- publishing privacy notice, consent manager obligations, handling data breach, data transfers and other facets. By setting out the requirements and enforcement mechanisms, these rules are aimed at helping businesses translate the regulatory obligations into functional compliance strategies.

However, certain elements still require more clarity like categorization of Data Fiduciaries (DFs) and Significant Data Fiduciaries (SDFs), data breach threshold, expected compliance timelines.

As we navigate this evolving regulatory landscape, it is important to first understand and break down these rules that would enable the organizations to build a foundation of a strong data protection framework.

01 NOTICE REQUIREMENTS

Draft DPDP rules mandate data fiduciaries to provide clear and independent notices to Data Principals when collecting their personal data. These notices should be written in plain and clear language and should provide details necessary to enable the Data Principal to give specific and informed consent for the processing of the personal data.

What needs to be in the notice?

Itemized description of the personal data collected.

Specific purposes for which the personal data is being collected and goods and services that would be provided.

Communication link for accessing the website or app for data principal to withdraw the given consent, exercise the rights under the act and a link to make compliant to the Board. Fiduciaries and Consent Managers will need to ensure that the consent withdrawal is as easy as taking the consent. The first step in operationalizing these rules for all the data fiduciaries would be to identify all personal data touch points and ensure that detailed notices are published at each stage of data collection.

Business contact information of the Data Protection Officer in case of a Significant Data Fiduciary, or an equivalent representative for regular Data Fiduciaries.

02 CONSENT MANAGERS

A unique aspect of the DPDP Act is the introduction of the Consent Manager, a concept not found in GDPR or other global data protection regulations. Recognizing the complexities of consent management for both Data Fiduciaries and Data Principals, the Indian government has introduced this intermediary layer to streamline the process. Consent Managers act as independent entities, enabling Data Principals to provide, manage, and withdraw consent seamlessly across multiple Fiduciaries through a unified interface. This approach not only simplifies compliance for organizations but also enhances user control over personal data, making consent management more transparent and efficient.

Who can be a Consent Manager

01
Company incorporated in India

02
Net Worth > = INR 2Cr

03
An entity with the technical, operational, and financial capacity to fulfill Consent Manager obligations

04
Need to be registered with the Board

03 KEY RESPONSIBILITIES OF A CONSENT MANAGER

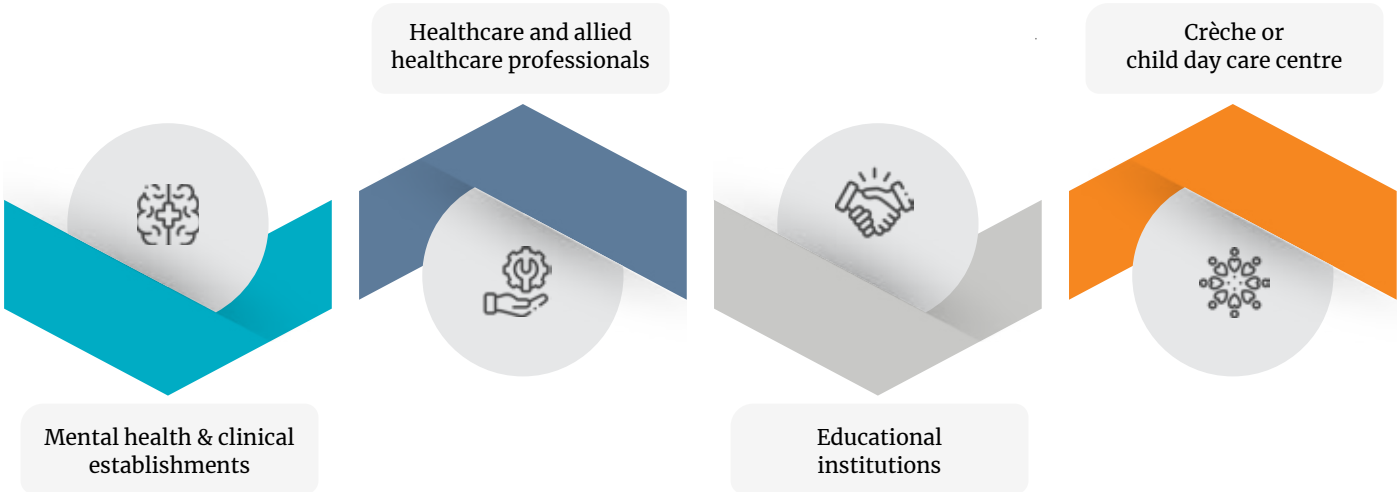
- Maintain a website and/or app as a primary interface for Data Principals.
- Act in a fiduciary capacity to facilitate consent management.
- Ensure data access and sharing in a non-readable format.
- Maintain consent records, including notices and data-sharing details.
- Provide records in a machine-readable format upon request.
- Retain consent records for a minimum of seven years.
- Implement security measures to prevent data breaches.
- Avoid conflicts of interest with Data Fiduciaries.
- Establish effective audit mechanisms for compliance monitoring

04 VERIFIABLE CONSENT

Under the draft rules, Verifiable Consent is a crucial element for ensuring that the rights of certain vulnerable groups, such as children or persons with disabilities, are adequately protected. To facilitate this, fiduciaries will need to have required technical and organizational measures in place to obtain valid consent from the parent or the legal guardian. Organizations have been relying on simple consent collection mechanisms for compliance, but not anymore as they will need to have an additional check to ensure that the consent they have obtained is verifiable. To capture the verifiable consent, organization can use virtual tokens or legal ID submission proofs that will verify the identity of the parent or guardian. Such due diligence safeguards the integrity of the consent process, ensuring that it is both informed and legally binding, particularly when dealing with sensitive personal data of vulnerable individuals. This approach aligns with the overarching goal of the DPDP Act to uphold data privacy while fostering trust between Data Fiduciaries and Data Principals.

It will be fascinating to observe how fiduciaries and consent managers implement innovative technologies to verify identities using virtual tokens or platforms like Digi Locker and making use of privacy-enhancing technologies (PETs) to safeguard personal data. With the upcoming wave of data protection regulation in India, PETs are sure to gain significant traction, offering an efficient way to streamline and build a strong privacy posture of the organizations. This is especially important for fiduciaries handling huge volume of personal data, as these technologies are build on 'Privacy by Design' principles that enables organizations become compliant while handling the complexities of huge data.

The rules have exempted following establishments from certain obligations related to consent when processing children's personal data



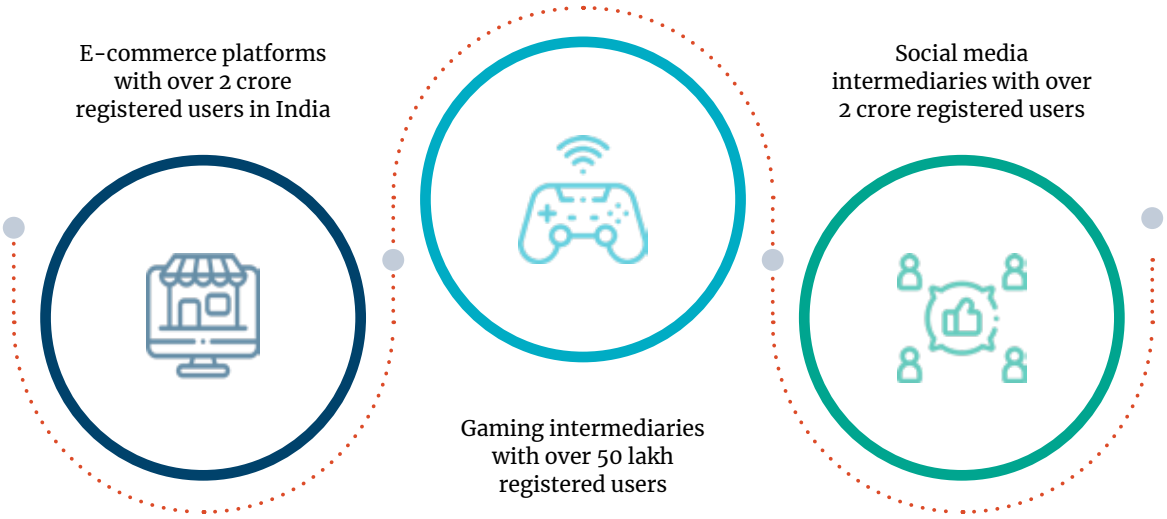
"While the rights of Data Principals are clearly outlined, these rules do not specify the timeline for fulfilling these rights and will further provide clarity to both data principals and data fiduciaries. Moreover, relying solely on online channels for raising such requests may not be sufficient, enabling telephonic mode for exercising the rights will ensure broader accessibility, including those less familiar with digital platforms, can effectively exercise their right to privacy."

05 RETENTION OF PERSONAL DATA

Data retention and safe disposal of personal data has been a critical concern for organizations as per CII - Protiviti State of Data Privacy" Survey Report 2024. Personal data cannot be retained indefinitely— and once the purpose for which the data was collected has been fulfilled, it must be securely disposed.

One of the key indicators of an organization's privacy maturity is a well-defined data retention and disposal process that ensures compliance with the applicable regulation along with reducing data processing and storage costs.

It is crucial for organizations to define retention schedule to ensure data is not over retained. However, the challenge arises because of varied legal and sectoral requirements for retention period and disposal. To simplify retention, the draft DPDP rules have defined retention limits for the following three categories of data fiduciaries:



These entities cannot retain personal data if a user has been inactive for more than three years, unless required by other regulations. Before deletion, users must be notified 48 hours in advance, allowing them to log in or initiate contact to retain their data.

> The draft DPDP rules does provide clarity for certain industries w.r.t. data retention, however the rules have not defined standardized retention limits for other industries. The onus has been left on the businesses to individually establish their own retention framework aligned with the draft DPDP rules and sector-specific regulations.
>
> However, greater clarity on the types of data that should be retained and for how long— even if not industry-specific— would help businesses ensure compliance while effectively managing data lifecycle risks. It will be interesting to see how organizations navigate these requirements to strike a balance between compliance, operational efficiency, and user expectations.

06 BREACH NOTIFICATION

The State of Data Privacy in India 2024 survey revealed that 52% of organizations experienced at least one data breach or unauthorized access incidents in the last five years, marking data breaches as a top privacy concern. The biggest challenge that organizations face is the inability to identify and detect breach and respond in a timely manner. Without the proper breach detection mechanism, many incidents often go unnoticed. However, organizations can no longer take this challenge lightly as the draft DPDP rules, requires data fiduciaries to promptly notify both affected Data Principals and the Data Protection Board. Hence, to mitigate risks and minimize potential harm while ensuring compliance with the regulation organizations must setup proper breach management systems and devise a comprehensive strategy to monitor, detect, respond and notify in case of data breaches.

Notifying Data Principals

Once a breach is detected, fiduciaries must immediately provide affected Data Principals with the following details via their registered user accounts:

- Nature, extent, timing, and location of the breach
- Potential consequences for Data Principals
- Measures taken by the organization to mitigate risks
- Recommended safety actions for Data Principals to minimize impact
- Contact details of the responsible person handling breach-related queries

Reporting to the Data Protection Board is to be done as follows:

1. Primary Intimation: Immediately notify the Board upon discovery, specifying the nature, extent, timing and location of the breach.
2. Comprehensive Report with additional breach details post the analysis by the organization within **72 hours** (Extensions may be granted in specific circumstances):
   - Detailed facts covering the breach, including events, root causes, and any other information
   - Mitigation strategies implemented or proposed
   - Identification of person involved in the breach, if possible
   - Remedial measures to prevent re-occurrence
   - Evidence of notifications sent to affected Data Principals

A clear definition of 'data breach' is currently lacking in the draft rules w.r.t. what is considered as a data breach in terms of volume of data or impact on the data principal to become reportable. A well-defined breach threshold criterion will aid businesses in assessing the breach incidents and report effectively.

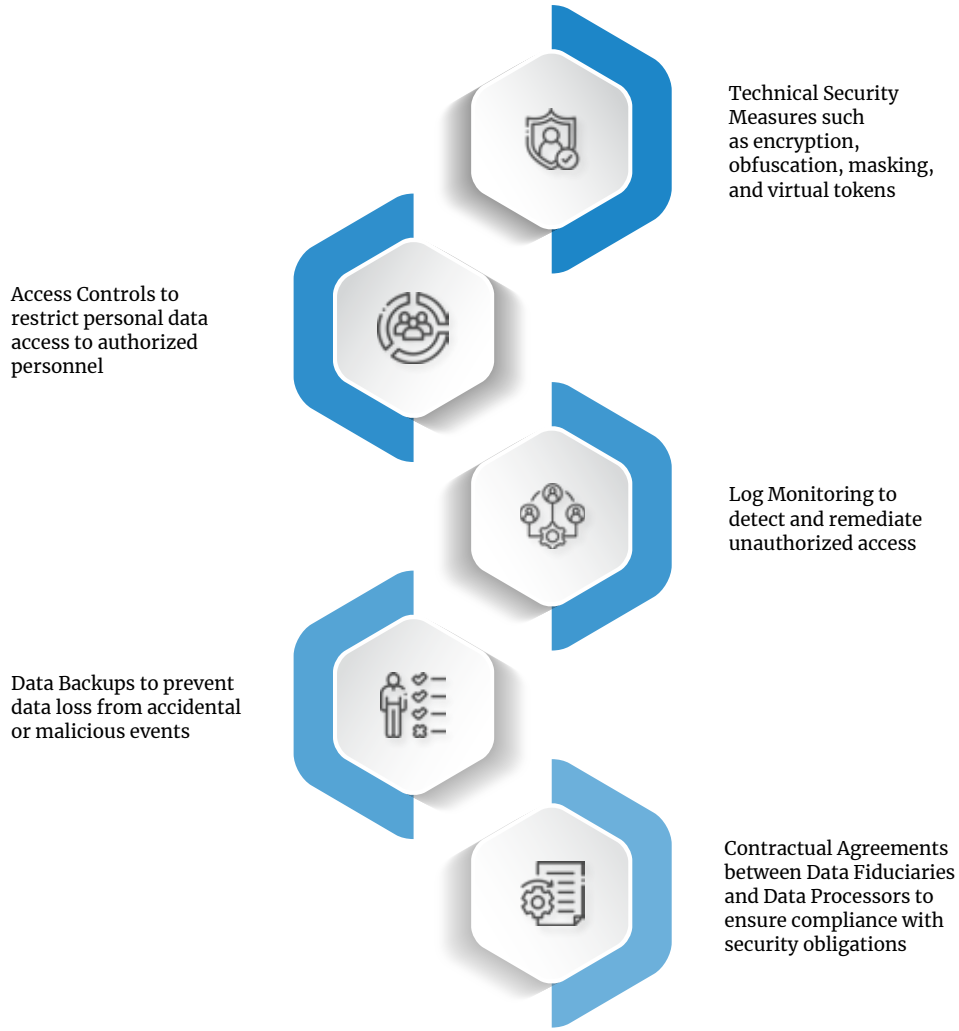
Until further clarity is provided, organizations must assume that any personal data loss could be considered a breach, requiring proactive compliance and risk management.

Additionally, the rule mandating breach notification to the Data Protection Board within 72 hours may be too stringent for organizations dealing with complex incidents. A phased reporting mechanism—initial notification followed by a detailed reporting—could be more practical.

07 SECURITY MEASURES

In our State of Data Privacy in India 2024 survey, we observed that larger organizations are more likely to have dedicated privacy offices and rely on their IT/IS and legal teams for data security. However, the draft rules help provide a clear framework for organizations of all sizes, guiding them on what can be done technically to protect personal data. These rules outline the minimum-security measures that must be implemented to safeguard personal data in possession or under control, as well as in the processing activities carried out by Data Processors on behalf of the Data Fiduciary.

The collaboration of various teams—privacy, IT, legal, and security—is essential in achieving compliance. The draft rules specify key security measures, including:



For smaller organizations, implementing robust measures will require some investments on strong data protections systems such as DLP (Data Loss Prevention), Access management systems, log monitoring tools.

Privacy-enhancing technologies (PETs) can be helpful in simplifying compliance while safeguarding personal data and bolstering data protection across organization.

08 / ENABLING RIGHTS OF DATA PRINCIPALS

To ensure transparency and provide better control of their personal data to the Data Principals, the draft DPDP rules empowers them with 4 Data Principal Rights:

Right to Access Information – Can request a copy of their personal data that is being processed, with details on how and where it is being used.

Right to Correction and Erasure – Can request corrections or updates to their personal data to ensure accuracy and completeness. Additionally, they can demand erasure if the data is no longer required for legal or business purposes.

Right to Grievance Redressal – Organizations must provide accessible and efficient grievance redressal mechanisms to address complaints related to data processing.

Right to Nominate – Data Principals can designate a nominee to exercise their rights in the event of their death or incapacity.

The responsibility to enable these rights lies with the fiduciaries and consent managers. They must ensure that the appropriate information is provided on their websites or apps to facilitate the exercise of all four rights. A customer verification mechanism should be in place to authenticate the identity of the Data Principal. For the Right to Grievance Redressal, organizations must establish a system with defined response timelines, alongside the timeline as to when they would implement the appropriate technical and organizational measures when responding to such request.

> “While the rights of Data Principals are clearly outlined, the draft rules do not specify the timelines for fulfilling these rights. Moreover, relying solely on online channels, such as websites or apps, may not be sufficient in India, where many individuals may not be familiar with digital platforms. Incorporating a telephonic mode for exercising these rights would ensure broader accessibility, allowing for discretion in determining the volume or impact that qualifies an incident as reportable.”

09 SIGNIFICANT DATA FIDUCIARY

The DPDP Act introduces a new category of Significant Data Fiduciaries (SDFs) based on factors such as data volume, risk to Data Principals, public order, potential impact on the sovereignty of India and other criteria. Though the rules do not specify the organizations or the industries that would be considered as SDFs but it is highly likely that financial institutions, social media platforms, healthcare providers and e-commerce companies will fall under this category.

Providing clarity on the factors with regard to quantification on volume or type of risks would enable businesses to assess their regulatory obligations in advance and start their compliance journey.

Organizations categorized as Significant Data Fiduciaries must fulfil stricter obligations, including:

- Appointing a Data Protection Officer (DPO)
- Conducting independent compliance audits
- Performing regular Data Protection Impact Assessments (DPIAs) and submitting key findings to the Board
- Ensuring algorithmic processing does not infringe upon Data Principal rights
- Restricting cross-border data transfers if mandated by the Indian government

"The rules empower the government to classify certain entities as Significant Data Fiduciaries but the absence of specific thresholds or criteria creates uncertainty. Clear, objective criteria would help organizations assess their obligations better.

Also, unlike the GDPR, which mandates DPIAs for high-risk processing, the draft DPDP rules lack clear triggers for when organizations must conduct them Defining triggers for when DPIAs need to be conducted would provide much more clarity to SFDs as to when they need to conduct the DPIA. Additionally, though DPDPA rules does not mandate data fiduciaries to conduct the assessment, but it should be a recommended practice irrespective of the fiduciary classification if the trigger criteria apply to the data fiduciary as well. The assessment is a mean to identify the risks in advance and implement mitigation measures when dealing with personal data.

Similarly, defining what constitutes a "significant observation" and setting thresholds for reporting findings would improve regulatory clarity.

Another key area for refinement is due diligence for algorithmic processing. Currently, this obligation is limited to SDFs, but with the growing adoption of AI/ML-driven data processing, all Data Fiduciaries should be required to assess and mitigate risks associated with automated decision-making. Again, applying these obligations to all kinds of data fiduciary would help ensure stronger oversight on usage of emerging technologies across all industries."

10 / DATA TRANSFERS

The cross-border data transfers under the draft DPDP Rules states allows central government to restrict data transfers on special orders when sharing data with foreign states or entities under their control when deemed necessary.

However, there is lack of clarity on the approach for data transfers like:

- Countries where data cannot be transferred due to lack of data protection regulations
- Countries where data can be transferred freely because of strong data protection regulations, similar to adequacy decision under GDPR
- Strong data transfer mechanisms for organizations to rely on like Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs)

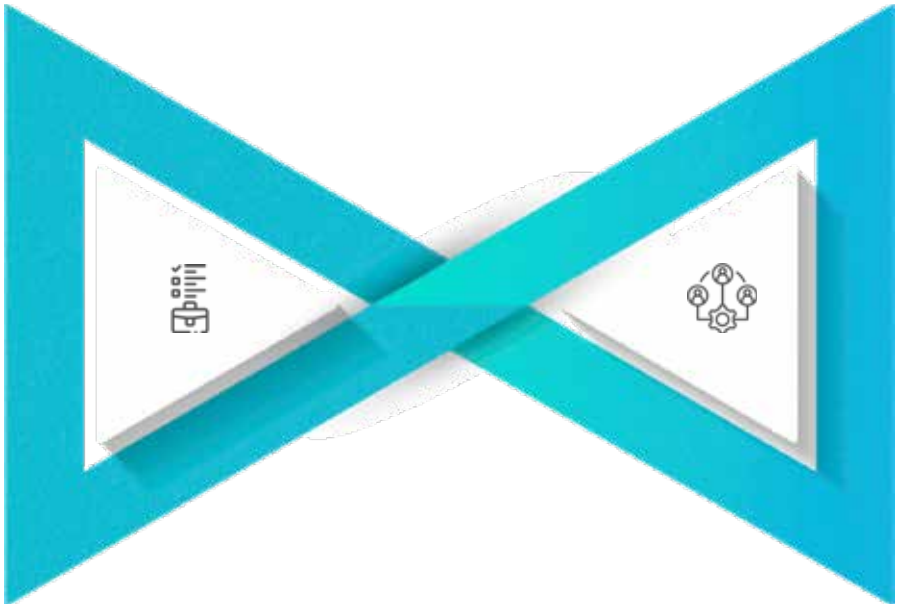
If stricter data localization requirements are enforced, it would drive investment in India's data infrastructure, especially for data center provides and global IT firms. The advantage for organizations relying on data localization will be risk mitigation arising from change in government policies related to cross border data transfers or sudden imposition on data transfer affecting its operations. It would be important to strike a balance between storing data locally and sharing data across borders to maintain our digital economy and global competitiveness.

> "On one hand where some sectoral regulations from bodies like the RBI mandates data localization for financial data, DPDPA takes a much open approach where data transfer can only be restricted on the notification of central government. Building a more structured approach to handle data transfers will provide better clarity to the organizations. Assessment frameworks similar to TIA and TRA can help organizations navigate the complexities of data transfers."

11 GOVERNMENT OVERSIGHT AND INFORMATION

The draft DPDP rules empower the Central Government to request necessary information from Data Fiduciaries and intermediaries for specific purposes under the Act. Rule 22 outlines that:

The government will define the timeframe for providing such information.



If the disclosure impacts India's sovereignty, integrity, or security, the Data Fiduciary or intermediary must not disclose the request without prior written approval from an authorized official.

Exemptions

While the draft DPDP rules framework establishes stringent obligations for Data Fiduciaries, certain exemptions have been outlined to facilitate essential functions such as research, healthcare, and child safety. These exemptions ensure that critical services remain unaffected while still upholding privacy principles.

RESEARCH, ARCHIVING AND STATISTICAL	The provisions of the act shall not apply to the processing of personal data necessary for research, archiving or statistical purposes.
HEALTHCARE	The provision of processing of children's data will not apply if processing is restricted to provision of health services to the child by such establishment or professional, to the extent necessary for the protection of her health.
EDUCATIONAL	The provision of processing of children's data processing is restricted to tracking and behavioural monitoring— (a) for the educational activities of such institution; or (b) in the interests of safety of children enrolled with such institution.
CRECHES	The provision of processing of children's data processing is restricted to tracking and behavioural monitoring in the interests of safety of children entrusted in the care of such institution, crèche or centre

12 CONCLUSION

While the draft rules provide much-required clarity on the regulatory facets such as privacy notices, establishing verifiable consent mechanisms, breach notification, and additional obligations of Significant Data Fiduciaries (SFDs), the key debate around key issues still remain open. The lack of clarity on data transfers, transfer assessment to identify risks and approved transfer mechanisms creates uncertainty for businesses managing global data flows.

Additionally, practical implementation of verifiable consent remains complex for both small and large organizations. Not to mention, the absence of expected implementation timelines adds to the uncertainty along with no clear guidance on the classification criteria for SDFs and Data Fiduciaries (DFs) making it difficult for organizations to proactively plan and begin their privacy compliance journey.

The public consultant on the rules provided the industry experts to voice their concerns and provide valuable inputs to further strengthen our privacy framework while sharing the nuances of practical implementation.

With the deadline for public consultation now closed, we are anticipating further clarity on the rules in the next few months.

However, organizations cannot sit back and relax and wait for the final rules. The time is to act now and get ahead in the compliance journey.

Proactively assessing their privacy posture and implementing foundational measures today will ensure they are well-prepared for the regulatory changes ahead. Building sustainable privacy programs that promote consumer trust and also strengthen data governance practices will provide strategic advantage to the organizations.

At Protiviti, we understand these challenges and are committed to being your trusted partner in this journey. With deep expertise in data protection, privacy consulting, and regulatory compliance, we help organizations navigate complexities by assessing their current privacy state, designing and implementing robust frameworks, operationalizing compliance measures, and leveraging advanced privacy technologies. By taking a strategic and proactive approach today, businesses can not only ensure compliance with the draft DPDP rules but also build a strong foundation for responsible data stewardship in an increasingly digital world—turning privacy into a competitive advantage rather than just a regulatory requirement.

PATH AHEAD

Developing a Robust Data Privacy Program

Key steps to attain compliance to Digital Personal Data Protection Act, 2023.

01 Appoint a competent person as data protection officer based in India and make the contact information available.

02 Seeking consent from the Data Principal and informing about the type and purpose of data collected.

03 Define privacy notice templates to be preceded or accompanied by consent requests.

04 Define and document privacy policies.

05 In case personal data transmission is required outside India, then an inventory of countries to which the transfer shall happen should be created. This can be validated once the central government defines the list of countries to which the data transfer is restricted.

06 Initiate implementation of the policies and procedures to enhance privacy landscape.

07 Define templates for responding to data principal rights requests related to the following:
- Data Fiduciary and Significant Data Fiduciary: Correction and erasure requests.
- Startups and other similar class of Data Fiduciary: Correction requests.

08 Define process for grievance redressal for data principals.

09 Ensure privacy enhancing technology (PETs) such as encryption, differential privacy and process relevant measures to strengthen privacy.

10 Have a data processer defined (in case required) but only after having the right safeguards and contract.

11 Define data breach notification related process and templates for the Data Privacy Board and the Data Principal.

12 Perform Data Protection Impact Assessment (DPIA).

13 Have an independent data auditor appointed for validating the compliance.

14 Perform periodic reviews.

DATA FIDUCIARY SIGNIFICANT DATA FIDUCIARY START-UPS AND OTHER SIMILAR CLASS OF DATA FIDUCIARIES

OUR RECENT REPORTS

INSIGHT

Navigating Data Privacy in Digital India

REPORT

State of Data Privacy in India

SURVEY REPORT

From AI To Cyber - Deconstructing A Complex Technology Risk Landscape

INSIGHT

Harnessing the future: Protiviti's research on AI adoption

WHITEPAPER

AI Driven Collections Strategy for Unsecured Lending

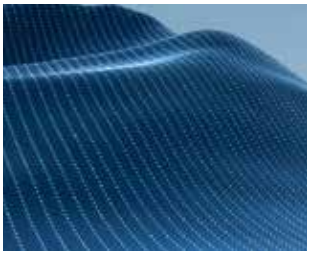
WHITEPAPER

ML Model Validation Best-practice

INSIGHT

Top compliance challenges facing the technology industry in 2025

INSIGHT



Technology-modernization projects

NEWSLETTER

The Directors Playbook for Gen AI

REPORT

AI Trends and Future Impact Industry Adoption & Insights

ABOUT **PROTIVITI**

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned member firms provide clients with consulting and managed solutions in finance, technology, operations, data, digital, legal, HR, risk and internal audit through a network of more than 90 offices in over 25 countries.

Named to the 2024 Fortune 100 Best Companies to Work For® list for the past 10 years, Protiviti has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti is a wholly owned subsidiary of Robert Half Inc. (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Sandeep Gupta
Managing Director
sandeep.gupta@protivitiglobal.in
+91 9702730000

Vaibhav Koul
Managing Director
vaibhav.koul@protivitiglobal.in
+91 9819751715

Aju Sebastian
Managing Director
aju.sebastian@protivitiglobal.in
+91 9818286225

Sarita Padmini
Senior Director
sarita.padmini@protivitiglobal.in
+91 9953043552

Sahil Chander
Senior Director
sahil.chander@protivitiglobal.in
+91 8800490154

Nagesh Akula
Senior Director
nagesh.akula@protivitiglobal.in
+91 9866694411

Acknowledgement

Vaishnavi Gautam from our Security & Privacy Solutions Practice have contributed to the publication.
Led by Vaibhav Koul & Sarita Padmini.

PROTIVITI INDIA **OFFICES**

Ahmedabad
6th Floor, West Gate, E-Block,
Near YMCA Club, SG Highway,
Gujarat, 380 015, India

Bengaluru
Umiya Business Bay - 1, 9th Floor
Cessna Business Park, Outer Ring
Road, Kadubeesanahalli, Varthur
Hobli Bengaluru – 560 049
Karnataka, India

Bhubaneswar
1st floor, Unit No 104, 105, 106
Utkal Signature, Chennai Kolkata
Highway Pahala, Bhubaneswar
Khordha - 752 101
Odisha, India

Chennai
10th Floor, Module No. 1007
D Block, North Side, Tidel Park
No. 4, Rajiv Gandhi, Salai,
Taramani, Chennai - 600 113
Tamil Nadu, India

Coimbatore
TICEL Bio Park, (1101 - 1104)
11th floor Somaiyapalyam
Village, Anna University Campus,
Maruthamalai Road, Coimbatore
North Taluk, Coimbatore – 641046
Tamil Nadu, India

Gurugram
15th & 16th Floor, Tower A,
DLF Building No. 5, DLF Phase III
DLF Cyber City,
Gurugram – 122 002
Haryana, India

Hyderabad
Q City, 4th Floor, Block B,
Survey No. 109, 110 & 111/2
Nanakramguda Village
Serilingampally Mandal, R.R.
District Hyderabad – 500 032
Telangana, India

Kolkata
PS Srijan Corporate Park,
Unit No. 1001 10th & 16th Floor,
Tower - 1, Plot No. 2 Block - EP &
GP Sector-V, Bidhannagar
Salt Lake Electronics Complex
Kolkata –700 091,
West Bengal, India

Mumbai
1st Floor, Godrej Coliseum
A & B Wing Somaiya Hospital Road
Sion (East) Mumbai – 400 022
Maharashtra, India

Noida
Windsor Grand, 14th & 16th Floor
1C, Sector - 126 Noida
Gautam Buddha Nagar- 201313
Uttar Pradesh, India

KS_Mar2025

Face the Future with Confidence®