pwc

# Readiness of India Inc. for the Digital Personal Data Protection Act, 2023: A PwC analysis

# Foreword

The Digital Personal Data Protection (DPDP) Act, 2023 ('Act'), is an important piece of legislation that is set to touch the lives of consumers, employees and business owners alike. It is expected to have a far-reaching impact on individuals, businesses and the overall economy.

For organisations in India, the Act is an opportunity to streamline their data collection and processes while enhancing customer confidence and overall stakeholder trust. The path towards that, however, has to be robust – with meticulous assessments and stock taking, comprehensive strategies, seamless execution even at the grassroots level, and diligent monitoring, reporting, and communication. How prepared are organisations in India to embark on this journey? What is the baseline from which they will have to steer towards compliance? Focusing on these pressing questions, PwC India set out to gauge where leading companies in India stand vvis-à-vis the 'new norm' laid down in the Act. The objective of our study was to examine the public-facing digital presence of Indian companies and evaluate their current state of operations to see if they align with the compliance expectations of the Act.

The results of our survey yielded some interesting insights. While most of the surveyed companies have taken small steps towards data privacy and ensuring the data rights of their customers, they seem to have a long journey ahead of them. Encouragingly, 90% of the organisations we evaluated were found to provide privacy notices to users. Many of these organisations either belong to regulated sectors or have a global presence, due to which they need to add a basic privacy notice across their online channels. Although most organisations showed the intent to do so, on assessing the comprehensiveness of these notices, we observed that the key elements of data privacy principles were to a significant extent. Only 9% of these companies sought consent that was freely given, specific and informed. Moreover, only 4% of these organisations were found to have a breach notification on their websites, and only 2% offered the option of multi-language consent.

Overall, this is a great opportunity for India Inc. to build trust, enhance its position among competitors and foster positive relationships with all stakeholders.

This study is a step towards furthering the discourse around data protection and privacy and building a data privacy culture within Indian organisations – as well as across the country.

Keeping in mind the wave of data protection and collaborative approaches adopted by organisations to move beyond 'privacy as an Act requirement' to 'privacy by design', this report also highlights the opportunities for India Inc. to contribute to digital India.

While the road ahead seems challenging, with the right vision, roadmap, strategy, ecosystem and partnerships, compliance with the clauses and provisions laid out in the Act can help in building globally competitive organisations that evoke trust and brand loyalty. The Act itself is progressive and adaptive – it is likely to stay relevant with changing times. The deftness, agility and resilience with which businesses achieve the goals defined in the DPDP Act will determine their ability to remain fit-for-future and contribute to India's journey towards becoming a mature digital and data economy.

I hope you will find this report to be informative and insightful.

**Sivarama Krishnan**
Partner and Leader – Risk Consulting, PwC India,
and Leader – APAC Cybersecurity and Privacy, PwC
sivarama.krishnan@pwc.com

# Table of contents

# Our study – setting the context

## The results of our study are presented and discussed in the following three sections:

| | |
|---|---|
| Section 1 | Outlines the need for our study, which aims to measure the current level of preparedness of organisations with respect to the DPDP Act. |
| Section 2 | Provides a high-level snapshot of the companies covered in this study. |
| Section 3 | Discusses the findings of our study, and also offers suggestions for improvement in select areas. |
| Appendix | Lays out the parameters for our assessment of company websites. |

In the past few years, digitisation in India has taken centre stage with efforts such as Digital India, which aims to provide Government services electronically, promote digital literacy and build digital infrastructure. E-governance initiatives such as DigiLocker and DigiYatra were part of the Digital India journey. Taking this journey forward, the Digital Personal Data Protection (DPDP) Bill received the president's assent to become an act on 12 August 2023. The Act will enable organisations in India to handle digital personal data responsibly while empowering individuals to control their own data.

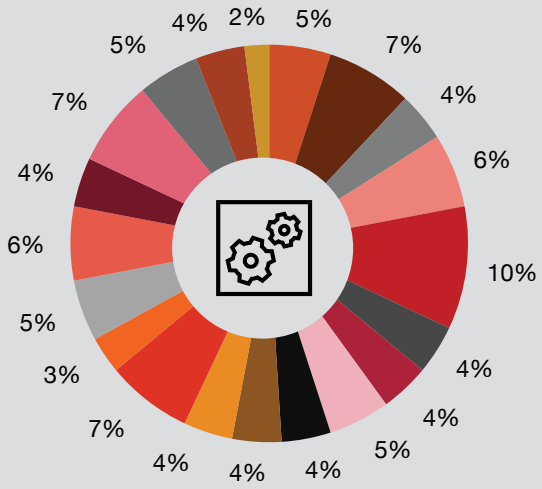
Given this context, PwC conducted a study to measure the current preparedness of organisations across various sectors in India with respect to the provisions of the Act. These organisations have public websites which are often reflections of the maturity of data privacy and protection controls that are implemented within the organisation. Several provisions of the DPDP Act are expected to be implemented in an organisation's website – namely privacy notice, cookie consent, parent or guardian consent for children below 18 years of age, and consent management, including opt in and opt out.

As part of this study, we assessed these websites to form a view on the level of preparedness of these organisations. In order to do so, we browsed these websites as an ordinary user and collated information by visiting various pages.

# Companies covered

We started by looking at the websites of 1,000 Indian companies to form an initial view. As the degree of maturity varied depending on the size of the organisation, we decided to do a deep dive of the websites of around 100 companies across sectors which were more likely to have embedded privacy features. This report used the checklist included in the appendix to assess a total of 100 companies – covering listed companies as well as educational institutions.

## Sector-wise distribution of the 100 companies assessed




- Aviation
- Banking
- Consumer
- E-commerce
- Education
- Energy
- FinTech
- Healthcare
- Hospitality
- Information technology
- Insurance
- Manufacturing
- Media (OTT)
- Pharma
- Realty
- Retail
- Start-ups
- Super apps
- Telecom
- Others

Note: The category 'Others' includes approximately 2 companies out of 100 spanning multiple sectors.

**Based on online presence, how does India Inc. fare with respect to the DPDP Act, 2023?**

- 90% of organisations provide a privacy notice to data principals when collecting data through their websites. Such a notice is the first step adopted by any organisation entering the digital world. Hence, the high level of compliance cannot be interpreted as an outcome of the privacy expectations from organisations.
- 9% of the forms that collect personal data on company websites obtain clear and explicit consent from data principals.
- 43% of organisations do not provide a well-defined purpose for which data is shared with third-party processors.
- 2% of these privacy policies or notices are in languages other than English.
- 54% of organisations mention their retention period, stating how long they will be retaining the data.
- 41% of privacy policies specify data principal rights (correction, access and erasure).
- 4% of organisations have published breach notification mechanisms on the website.

The banking, FinTech and insurance sectors have historically been heavily regulated owing to the Reserve Bank of India's guidelines, which is evidenced by this report. These sectors are in a slightly better position to respond to DPDP requirements at their end due to limited sectorial regulation expectations in terms of data processing. Therefore, whether it is data sensitivity or technology adoption, these sectors are likely to overtake others in implementing the expected controls of the Act.

# Our findings

**Most organisations are facing challenges in addressing privacy concerns,** though some may adapt faster due to past groundwork.

**An encouraging 90% were found to provide privacy notices to users. Many of these organisations either belong to regulated sectors or have a global presence, and hence they need to add the basic principle of notice across their online presence.** If we go down a level to assess the comprehensiveness of notices, we observe key elements – purpose of processing, categories of data processed, retention period, principal rights and third-party sharing purposes – to be missing. Thus, the notices are not in line with the expectations of the Act.

**Consent that was free, specific and informed was sought by only 9% of organisations – primarily in the regulated sector.** This low percentage indicates that additional efforts are needed in this area, as consent forms the legal basis for processing personal information. We found the practice of taking bundled consent to be prevalent, with the assumption that accessing a home page may be considered consent. Cookie consent was limited to 16% of organisations, while the option to withdraw consent was offered by 48%. Further, only 2% of these organisations provided multilingual consent. Therefore, the consent ecosystem – consent management platform, cookie consent, integration with consent managers – is a great opportunity for India Inc. to invest in, from both people and technology viewpoints.

**Data principal rights were mentioned by 41% of organisations,** mainly in sectors such as information technology, hospitality, consumer and pharma. This indicates that these organisations have proactively taken initial steps and enabled mechanisms to uphold data principal rights. Other sectors will have to follow suit to meet the compliance requirements of the Act.

**Only 4% of organisations were found to have a breach notification in place, which may also be construed as non-compliance with a few sectoral regulations.** FinTech organisations seem to have the highest level of preparedness in this regard.

**About 74% of organisations share contact details of a person or an office that can be contacted for data privacy queries.** These organisations mostly belonged to the technology, banking, healthcare, and pharma sectors. However, 17% of organisations have listed an email address for customer care or other functions to which queries on data protection may be directed. Furthermore, 57% of organisations have proactively provided the contact details of their data protection officer (DPO)/privacy office.

Organisations may consider appointing a DPO to help achieve overall compliance, even if they aren't categorised as significant data fiduciaries.

**Children's personal data** has been given a special focus in the Act. We found that there was very limited segregation of children's information. Age, which is a qualifying criterion, was not captured while availing many digital services. This means that in such cases, verifiable parental consent was also not obtained. Therefore, capturing age and eventually embedding additional controls for parental or guardian consent will be an important area of focus for direct consumer-facing organisations.

## A. Consent

**Transparent consent is key to building trust with data principals for sharing their data, leading to a mutual exchange of value.**

**Organisations should develop or establish robust and user-centric consent management mechanisms to build and maintain customer trust.**

Consent is the approval given by the data principal to collect and process their personal data for specific purposes. Thus, organisations should implement practices such as displaying clear and concise consent requests, offering options to opt in or opt out, and ensuring ease of withdrawal of consent for their website users.

- 9% of organisations collect consent which can be considered free, specific and informed. In such cases, mainly bundled consent is collected (i.e. single consent is obtained for multiple purposes).
- 48% of organisations provide the option to withdraw consent. However, the process of withdrawing consent is not as easy as providing it.
- Consent is **obtained in multiple regional languages only by 2% of organisations.**

A consent manager can help organisations manage the complexities that come with enabling the rights of individuals to manage their consent.

### Current practices

- Just proceeding to a website or app's home page is considered as consent: **'By proceeding, you agree to our privacy policy, user agreement and T&Cs.'**
- Consent is not always accompanied **by a notice stating why it is being captured.**
- Obtaining basic information about the service or product is **conditional** to providing consent.
- Although consent is **treated as a one-time agreement,** organisations often take it as a perpetual one.

**Way forward to comply with consent requirements**

**1. Audit existing data practices**

- Conduct a thorough assessment of existing touchpoints where data is collected, processed and stored.
- Evaluate the organisational need at both the technical and process levels for consent.

**2. Transparent privacy notice**

- Create a transparent privacy notice that clearly outlines what data is collected, why it is collected, how it is used and with whom it will be shared. This will help users to make an informed decision.
- Ensure that the notice is available in multiple languages.

**3. Integrate privacy considerations**

- Integrate privacy considerations into the design of products and services right from their conceptualisation.
- Design user-friendly interfaces like checkboxes and sliders to facilitate user choice for consent.
- Incorporate age verification for children (age <18) and parental consent.

**4. Consent options**

- Obtain consent clearly and freely.
- Provide granular consent options for users.
- Ensure that consent revocation is easy and straightforward.

**5. Consent managers**

- Establish a unified process for dealing with consent managers.

### Cookies

**Most websites use cookies to save information about users visiting the website.** Cookies are text files that are placed on a web browser to store user data like webpages visited, items in the cart and log-in credentials. These are widely used to provide a personalised experience to website users.

Obtaining cookie consent is a crucial aspect of online interactions. Organisations should obtain cookie consent via their websites to inform data principals visiting their website about the personal data collection by cookies.

- 16% of organisational websites display a cookie consent banner to users highlighting that their personal data would be collected and processed by the organisation.
- 33% of organisations display a cookie notice informing users that the website (or any third-party service used by the website) they are navigating uses cookies.

**Presently, the information technology, hospitality and aviation sectors** are ahead in terms of obtaining cookie consent and giving users control over their online experiences. This is because organisations from these sectors have a global presence, and most of them are compliant with data protection regulations around the world.

### Current practices

- Many organisations have not identified the retention period for cookie data – i.e. **cookie expiry is not specified.**
- Few websites provide details of cookie categories – e.g. first-party or third-party cookies.
- An **easy opt-out mechanism** that allows users to withdraw their consent and manage their cookie preferences is **not present** in most websites.
- Not many websites allow users to permit only **strictly necessary cookies.**

**Way forward to eliminate privacy concerns related to cookies**

1. Cookie consent banner

- Websites shall have a cookie consent banner that clearly informs users about the use of cookies.
- Cookies shall only be allowed after the user has provided their consent for the same.
- Consent checkboxes must not be pre-checked.

2. Strictly necessary cookies

- The website shall allow users to permit only strictly necessary cookies.

3. Cookie notice

**Websites shall include a cookie notice or disclaimer which must:**

- inform users that the website (or any third-party service used by the website) uses cookies
- clearly state which action will signify consent
- be sufficiently conspicuous to make it noticeable
- link to a cookie policy or make details of cookies' purposes, usage and related third-party activities available to the user
- specify the period of validity of cookies or mention the expiry period.

4. Easy opt-out mechanism

- Websites should include an easy-to-use opt-out mechanism that allows users to withdraw their consent and manage their cookie preferences.

5. Limiting the use

- The use of cookies should be limited only to purposes essential for the website's proper functioning. Using cookies for unnecessary tracking or data collection must be avoided.

## B. Privacy notice

**Privacy notices ensure transparency with data principals visiting a website and empower them to make an informed decision.**

**Organisations should have a comprehensive privacy notice on their websites.**

The privacy notice on a website should contain details about the personal data to be processed, purpose of processing, rights of data principals and ways in which they may be exercised. It should also include the manner in which the data principal may make a complaint to the board in case of any dispute.

- 90% of organisations provide a privacy notice to data principals when collecting data through their websites.
- 80% of organisations mention what personal data is collected by them in their privacy notice.
- 54% of organisations, which is around half of those having a privacy notice, mention the period for which personal data will be retained.
- 2% of organisations provide privacy policies or notices in multiple languages.

The Act expects organisations to provide notices in English or any of the languages specified in eighth schedule of the constitution. This clearly indicates the law's objective that everyone should be able to comprehend notices without any language barriers.

### Current practices

- Privacy notices are lengthy and filled with technical and legal jargon, instead of being simple and easy to understand.
- Privacy notices are not easily accessible from the website's main page, and users often struggle to find the same.
- Provisions such as mechanisms to lodge a complaint with the supervisory authority (board) need to be included.

**Privacy notice considerations for organisations**

1. **Data collection, purpose and legitimate use**
   - Data collected, its type and category
   - Clarity on why data is being collected and the purpose for which it will be used
   - Definition of legitimate use
   - Retention period
2. **Data sharing and transfer**
   - Recipients – e.g. third party, vendors
   - Details of cross-border transfers
3. **Data principal rights**
   - Data principal rights and mechanisms to exercise them
   - Mechanisms for making complaints to the board
4. **Contact details of the privacy office/point of contact**
   - DPO or data privacy office contact details
5. **Data protection measures**
   - Breach notification measures
   - Details of security safeguards in place

## C. Data principal rights

**Data principal rights are designed to give individuals control over their personal data and hold organisations accountable for how they handle that data.**

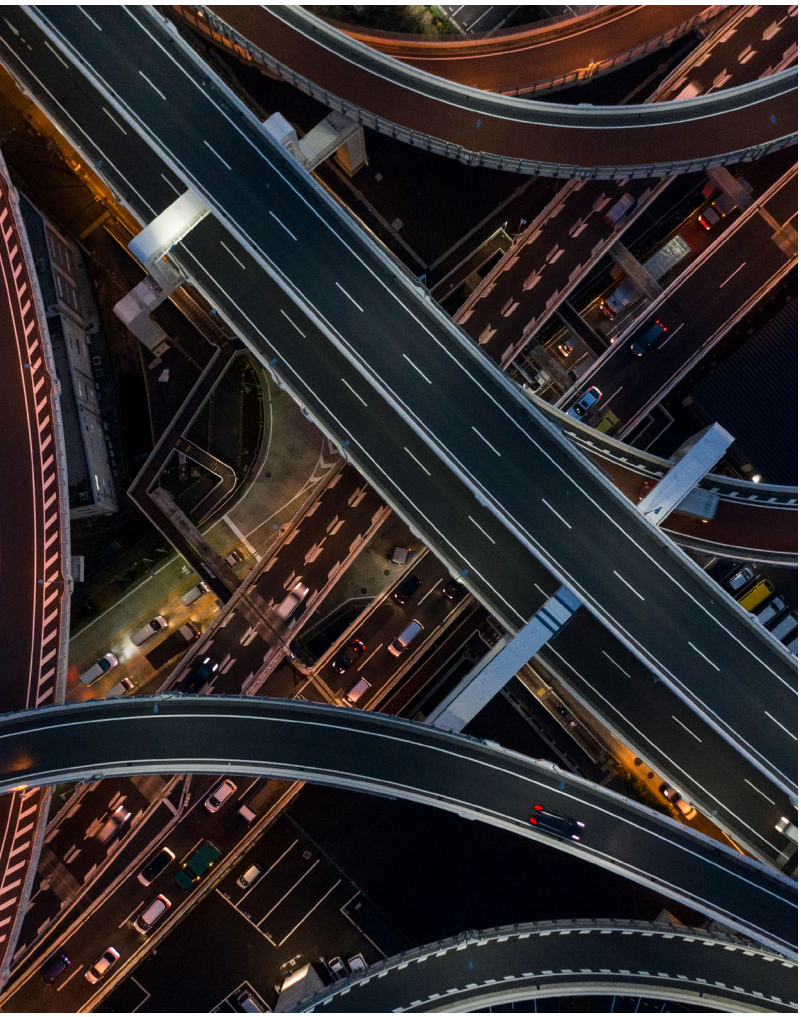
**By satisfying the requirements for data subject rights under the DPDP Act, organisations can demonstrate respect for the rights of individuals.**

It's important for organisations to be aware of these rights, establish processes to address data principal requests and ensure compliance with the DPDP Act.

- 41% of organisations display the rights of data principals (erasures, access and correction) on their website along with the mechanisms to exercise them.

While most organisations in the information technology, hospitality, consumer and pharma sectors and super apps have processes in place to honour data subject rights, they do not provide dedicated email addresses or online forms for support.

This represents an opportunity for organisations to invest in digital infrastructure that supports traceability across the complete data lifecycle – collection, storage and data in transit. Investing in such infrastructure will provide a pathway for consent managers to operate effectively and efficiently.



### Current practices

- Data principal rights are often buried within a lengthy privacy policy, making it difficult for users to find the same.
- There's a lack of clear instructions on how to exercise the rights or whom to contact for assistance.
- Websites omit certain data principal rights from their policy, leaving users unaware of the full range of rights they possess.
- Complex language and legal terminology used by websites can be confusing for users.

**Way forward for comprehensive data principal rights management**

1. **Establish a data principal rights policy**

- Develop clear and documented policies and procedures that outline how the organisation will handle data principal requests, including processes for verifying identity, responding within specified timeframes and maintaining request records.

2. **Update notice**

- Review and update privacy notices or policies to include clear information about data subject rights, how they may be exercised and the organisation's contact details for such requests.

3. **Establish communication channels**

- Set up dedicated channels, such as email addresses or online forms, through which data principals can submit requests and inquiries regarding their data rights.

4. **Leverage technology**

- Use tools for data inventories to understand what personal data they collect, where it is stored and how it is processed. This will help in responding to DSR requests in a timely and efficiently manner.

5. **Data retention requirements**

- Understand data retention and deletion requirements for the concerned sector or organisation so that even if a data principal asks for data erasure, the organisation has a valid reason to retain the data.

## D. Breach notification

**Organisations should ensure that there are robust breach detection, investigation, and internal and external reporting procedures in place.**

**They should design processes so that breaches are reported in a timely manner to the board and affected data principals.**

Having a well-defined breach management process in place is crucial for reducing the financial, reputational and legal risks associated with privacy breaches. This will help organisations respond quickly and effectively to data breaches, which is essential in today's digital landscape.

Robust breach investigation and internal and external breach reporting mechanisms should be part of the breach management process.

- Only 4% of organisations have proactively published a breach notification mechanism on their website. This will help them comply with the requirements of the Act.

We noted that organisations from the information technology and FinTech sectors have breach notifications in place. This is because they have a presence in countries with stringent data privacy laws and are already compliant with them.

### How organisations should prepare for reporting breaches

- Organisations should define what constitutes a personal data breach, as it does not include only loss of personal data.
- An internal breach reporting procedure should be put in place.
- Breach investigations are required to be carried out to assess the impact of personal data breach – e.g. number of data principals affected.
- A mechanism to notify the board and data principals in a timely manner should be put in place.

**Way forward for well-structured breach management**

1. **Detection and identification**
   - Detect that a data privacy breach has occurred.
   - Install breach monitoring systems and processes to identify if a breach is a security or data privacy breach.
2. **Assessment**
   - Conduct a thorough assessment of the breach to understand its extent and impact.
   - Determine the types of data that were compromised, potential risks to affected individuals and technical details of the breach.
3. **Notification**
   - Notify affected individuals, customers, partners, regulatory authorities and law enforcement agencies.
   - Communicate in a timely and transparent manner to avoid huge fines up to INR 250 crore. Develop a communication plan to keep stakeholders informed about the breach, its impact and the steps being taken to address it.
4. **Remediation**
   - Once the breach is contained, take corrective actions to address vulnerabilities or weaknesses that allowed it to occur.
   - Implement new security measures.
5. **Continuous monitoring**
   - Continuously monitor the security posture to prevent future breaches.
   - Adjust security strategies as needed.
   - Enhance employee training.

## E. DPO

**A DPO plays a key role in overseeing a company's data protection strategy and works with the technology and business functions to ensure its implementation.**

**Organisations, despite not being a significant data fiduciary, may appoint a DPO to oversee their data protection strategy and implementation.**

With the DPDP Act, 2023, the role of a DPO has come into sharp focus. A significant data fiduciary will have to appoint a DPO whose primary role is to ensure that the organisation processes the personal data of all its data principals in accordance with the Act. In addition to significant data fiduciaries, many other organisations, especially those processing large amounts of personal data or particularly sensitive data, may voluntarily appoint a DPO.

We looked at multiple websites to see if India Inc. is proactively mentioning the contact details of its DPO.

- Around 74% of organisations have listed contact details of a person or a team that can be contacted for queries around data processing.
  - 54% organisations of these organisations have proactively provided the contact details of their DPO. These organisations are likely to have a privacy framework in place, and they may have a head start in their compliance journey with the DPDP Act.
  - 17% of organisations have listed the email IDs of customer care or other functions for queries with respect to data protection. Although they may have customised their privacy notices, they do not have a supporting framework in place.

The Act expects organisations to provide notices in English or any of the languages specified in the eighth schedule of the constitution. This clearly indicates the law's objective that everyone should be able to comprehend notices without any language barriers.

**DPDP Act requirements on DPO**

- Should be based in India.
- Would represent the significant data fiduciary.
- Would report to the board of directors or a similar governing body.
- Would be the point of contact for the grievance redressal mechanism.

**Way forward to implement a DPO function**

1. Understand the applicability and scope
   - A significant data fiduciary would mandatorily need a full-time DPO.
   - Other data fiduciaries can voluntarily have one, depending on the nature of the data.
2. Build a data privacy organisation
   - A data privacy organisation is required to support the DPO.
     - Define the composition of the DPO team, consisting of data privacy coordinators and data owners from different functions.
     - Define roles and responsibilities, metrics and key performance indicators (KPIs).
     - Align with functions such as risk, legal and cyber.
3. Position the DPO correctly
   - Place the DPO correctly so that he/she can operate in an independent and transparent manner, reporting to the board of directors or an equivalent level.
4. Facilitate DPO functions
   - Create an environment where the DPO can carry out responsibilities effectively to ensure compliance.
5. Refer to Government or board updates
   - Continue to support the DPO.
   - Refer to Government notifications or updates from the data protection board.

## F. Data retention

**Data retention policies are essential for data privacy practices, as they dictate how long an organisation can retain personal data.**

**Organisations should determine the retention period based on operational, legal and regulatory requirements.**

Data retention refers to the practice of storing and maintaining data for a specific period of time. Personal data should be erased once the specified purpose is no longer being served, or a data principal withdraws consent – whichever is earlier.

- 54% of organisations, predominantly from sectors such as FinTech, e-commerce and information technology, and other regulated sectors (banking, insurance and aviation) state the retention period on their websites.

However, organisations from consumer, retail, realty and manufacturing need to define data retention periods and guidelines in line with the data privacy principles and legal requirements.

Organisations that retain data longer than necessary can create privacy risks for themselves, as this increases the potential for data breach or misuse.

### Current practices

- Retention period obligations are mentioned in the privacy notice or policies.
- Organisations are keeping personal data for longer periods than required.
- There is a lack of periodic reviews and practices such as anonymisation.
- Organisations are not keeping track of data principals who have been inactive for a significant period and are thus possible candidates for erasure.

**Way forward for identify data retention period**

**1. Data categorisation**

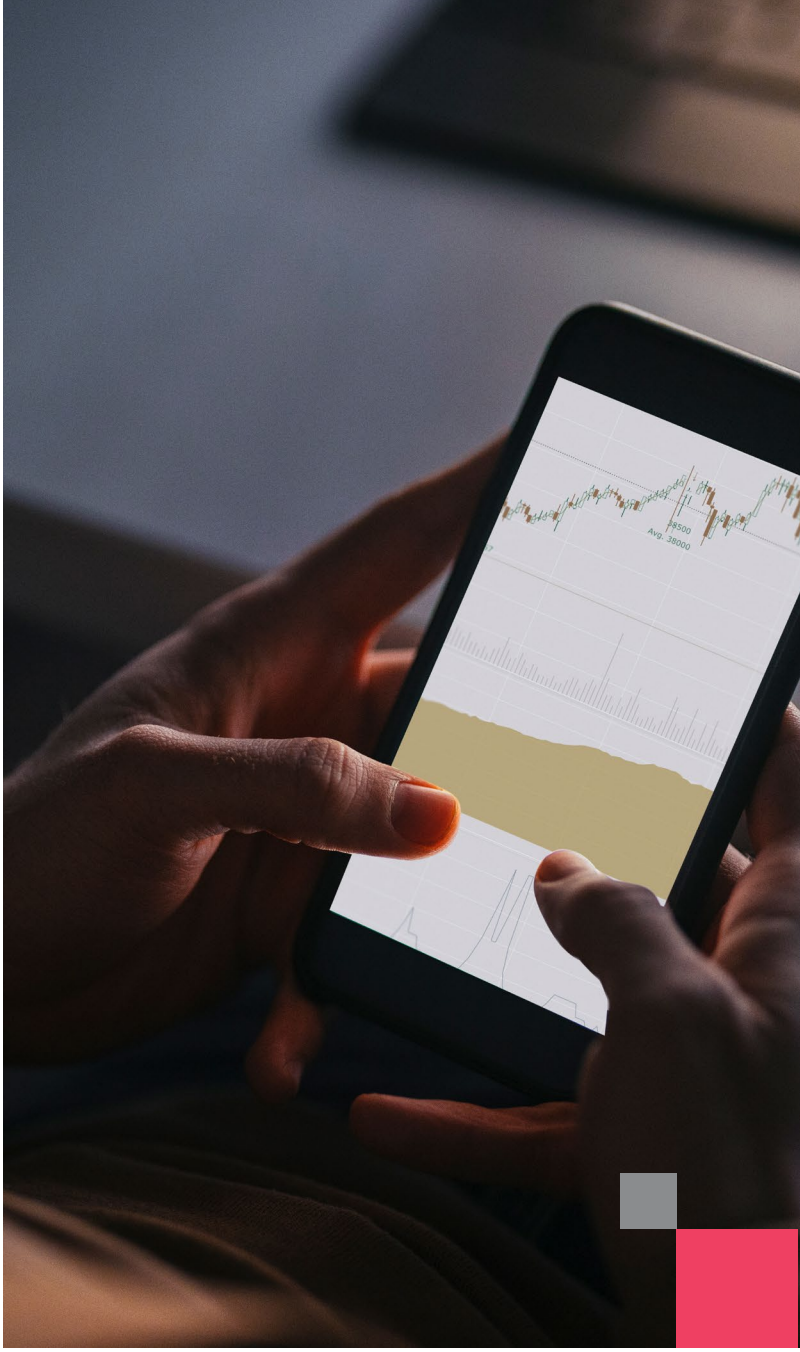
- Categorise data that the organisation collects and processes (financial records, employee data, marketing etc.).

**2. Legal requirements/best practices**

- Understand legal and regulatory requirements with respect to each category.
- Refer to industry standards for benchmarking.

**3. Assess business usage**

- Assess business needs and analyse business use.



**4. Retention policies**

- Develop retention policies for each category – involve legal and compliance in this process.

**5. Communicate and continue to document**

- Communicate internally and externally.
- Continue effective documentation of the retention period and related information such as data categories, data ownership and basis of retention.

## G. Third-party transfers

**Organisations must be transparent, accountable and vigilant when engaging in third-party data-sharing activities to ensure that personal data is handled in a lawful and secure manner.**

**Organisations should control third-party (data processors') personal data processing to ensure it is securely done and for given purposes.**

- 43% of organisations do not provide well-defined purposes for which personal data is shared with data processors for processing.

Within their website privacy notice on sharing of personal data, organisations often specify purposes that are either generic or do not provide transparency to the data principal.

While data processors are bound by agreement with the respective data fiduciaries, the DPDP Act, 2023, places the liability of protecting the personal data shared with such data processors on the data fiduciary themselves.

### Current practices

- Generic third-party statements are included within the data privacy notice on websites.
- Limited transparency on personal data being shared with data processors – e.g. an e-commerce company shares customer purchase history with a third-party analytics firm but does not disclose how the firm uses this data.
- Limited visibility for data fiduciaries into the processing practices undertaken by data processors.

**Way forward with third-party transfers (data processors)**

1. **Contractual agreements**
   - Establish clear and robust contractual agreements with data processors.
   - Outline data privacy obligations, security measures and compliance with the DPDP Act.
2. **Data mapping and inventory**
   - Conduct a thorough data mapping and inventory exercise to identify all data flows, including identification of data processors.
3. **Data principal rights**
   - Ensure data processors cease processing when consent is withdrawn by the data principal.
   - Ensure erasure of personal data by data processor post completion of specified purpose.
4. **Data security**
   - Implement robust security measures to protect personal data during transfers and ensure data processors implement adequate controls as well.
5. **Periodic checks and reviews**
   - Conduct periodic reviews and checks on the data processor's environment to ensure personal data processing is aligned with the DPDP Act.

## H. Children's personal data

**Protecting the privacy of children's personal information is essential to ensure their safety and well-being online.**

**Organisations need to implement strict data protection measures and parental consent for safeguarding children's data.**

An individual who has not completed the age of 18 years is considered a child as per this act. Organisations that handle children's personal data, whether through websites, apps or other digital means, are subject to legal obligations aimed at protecting the privacy and safety of children online. Such organisations may be tagged as a significant data fiduciary by the Central Government.

**Our research on Indian schools revealed the following:**

- One out of ten schools provides a privacy notice customised to children and does age verification to check if a user is a minor. Such schools state that they process children's data only after taking parental or guardian consent.
- Online services and product providers do not provide age-appropriate notices in a simple, visual and understandable format.
- Age, which is a qualifying criteria, is not captured when users avail many digital services. This indicates the absence of parental consent.
- Organisations provide personalised ads.
- Organisations do not assess the risks with respect to well-being of children in relation to their data processing.

**DPDP requirements for processing children's data**

- For processing the personal data of a child or a person with disability, verifiable consent of the parent or lawful guardian is required.
- Tracking or behavioural monitoring of children or targeted advertising directed at children is not allowed.
- Any processing of personal data that is likely to have a detrimental effect on the well-being of a child is restricted.

**Steps to ensure protection of children's data**

1. **Identify minors (Age <18)**
   - Age of the user of the product or service should be captured to identify if the user is below 18 years.
2. **Refresh notice or privacy policy**
   - Maintain easily accessible and understandable privacy policies that outline how children's data is collected, used and shared.
3. **Verifiable parental or guardian consent**
   - Obtain verifiable parental or guardian consent before collecting any personal data from children.
   - Offer parents the ability to review, modify or delete their child's data.
4. **Identify and address risks**
   - Perform a data protection impact assessment (DPIA) to assess risk to children's data processing.
   - Identify and address high-risk scenarios, e.g. tracking, behavioural monitoring or targeted advertising using children's data.
5. **Strengthen measures to protect children's data**
   - Incorporate privacy by design principles into development of digital products and services for children.
   - Implement robust security measures to protect children's data from unauthorised access or breaches.

# Appendix

The research factored in the following provisions of the DPDP Act, 2023, to assess the readiness of the India Inc.

### 1. Privacy policy and consent

- Do all the touchpoints of data collection (websites, online forms) have a provision for seeking customer consent?
- Is the privacy policy available in English only or is it available in any other language?
- Does the privacy policy mention the type of personal data collected?

### 2. Cookie consent

- Is cookie consent obtained (accept or deny) when the data principal visits the website?
- Does the website specify how it uses personal data?
- Does the cookie notice specify the cookie expiry timelines so that the user is aware of how long his data is retained?

### 3. Data principal rights

- Does the privacy notice or policy include data principal rights?
- Is consent withdrawal or the ability to opt out included in the privacy policy?
- Does the privacy notice or policy call out how data principals can exercise their duties?

### 4. Breach notification

- Is there a section within the notice that the data principals will be informed in case of a data breach?

### 5. DPO

- Are the name and contact details of the DPO or data privacy office published on the website?
- Are is the name and contact details of the Grievance Officer published on the website?

### 6. Data retention

- Does the website mention the retention period for personal data collected in the privacy notice, retention policy or any other document?
- Does the website specify that the personal data collected is being retained only for the time necessary for the purpose for which the data was collected and processed?

### 7. Third party

- Does the privacy policy include information about sharing of personal data with third parties?
- Is the purpose for third-party sharing specific or generic?

### 8. Children's personal data

- Is the privacy notice customised to state that children's personal data might be collected?
- Is parental or guardian consent obtained when the data principal visits the website?

# About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 152 countries with over 328,000 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,
and Leader – APAC Cybersecurity and Privacy, PwC
sivarama.krishnan@pwc.com

**Anirban Sengupta**
Partner and Leader, Business Risk Consulting
PwC India
Email: anirban.sengupta@pwc.com

**Anshul Jain**
Partner, Regulatory Services
PwC India
Email: jain.anshul@pwc.com

**Sundareshwar Krishnamurthy**
Partner and Leader, Cybersecurity
PwC India
Email: sundareshwar.krishnamurthy@pwc.com

**Heena Vazirani**
Partner, Business Risk Consulting
PwC India
Email: heena.vazirani@pwc.com

# Editorial support

**Dion D'Souza**

**Rashi Gupta**

# Design

**Shipra Gupta**

pwc.in

Data Classification: DC0 (Public)



SG/September 2023 - M&C 32092