Deloitte.

Confederation of Indian Industry

The DPDP Act and enterprises in India: Privacy for the board

April 2024

Table of contents

Foreword by CII

With increased digitisation of markets and other technological developments, processing of personally identifiable data has become integral to the business operations of many business entities today. Privacy of individuals has been recognised as a fundamental right in the landmark judgment of Supreme Court [*Justice K.S. Puttaswamy (Retd) vs. Union of India* W.P. (Civil) No 494 of 2012, Supreme Court of India, August 24, 2017].

Unchecked storing, use, processing of personally identifiable data may lead to adverse consequences for individuals in terms of financial loss, profiling, reputational loss, etc. Globally, risk of digitisation in terms of compromise with data privacy has long been identified and significant steps taken towards development of laws to protect data privacy rights. General Data Protection Regulation (GDPR) norms legislated in European Union (EU) is one such notable statute worldwide. In India, the Digital Personal Data Protection Act, 2023 (DPDP Act) has been enacted in August 2023, with an aim to curb and regulate the negative implications on data privacy.

The enactment of DPDP Act requires entities to rewire their business operations, processes, and strategies to ensure compliance with this new law in letter and essence. This will broadly come in the ambit of sound corporate governance as well since privacy of data and minimisation of data breach also result in substantial trust building amongst an entity's stakeholders. As a governance imperative, it requires boards of companies to take the lead in comprehending the law and ensuring that the statutory/compliance requirements percolate down in the organisation at all levels and across all functions uniformly. Boards will also need to ensure that the basic principles of protection of data and prevention of its misuse/ unauthorised use become the culture of the organisation and a non-negotiable function.

From the board's point of view, DPDP Act calls for a number of significant actionable steps, such as identifying the exact impact of the law on the entity, governance mechanism to be devised to ensure compliance, processes for smooth implementation, monitoring mechanism, identifying level of awareness within the entity and measures to increase awareness, how to engrain it in entity's culture, third-party risk management, risk mitigation plan, escalation matrix and how can data privacy imperative be used to build stakeholder trust.

CII has been a proponent of good governance practices and continues to focus on driving various initiatives with an aim to promote good corporate governance practices. CII considers compliance with applicable laws and regulations of the country as an imperative for all business entities. CII encourages its members to focus on long-term value creation by adopting sound governance practices which ensure continued success of businesses.

We hope that this publication on the "DPDP Act and enterprises in India: Privacy for the board" will enable businesses and boards ensure smooth transition, eased and timely compliance with the new law.

Foreword by Deloitte

In today's digital age, data is defining businesses. Enterprises across the globe, both private and public, have realised that data can be used to provide people with unique services and experiences. As the dependence on data grows to facilitate innovation, it is more important than ever to safeguard personal data and promote responsible handling.

To cater to the sensitive balance between individual rights and technological innovation, the Indian government has enacted the Digital Personal Data Protection Act (DPDP Act) in 2023. The provisions of this landmark legislation will pave the path for transformation in the digital governance landscape in India as the new law imposes obligations on enterprises that handle personal data.

As enterprises navigate the implications of the DPDP Act, it is essential that the board takes a proactive approach towards addressing both the opportunities and challenges that lie ahead.

The board can play a critical role in championing the implementation of the data privacy programme within their enterprise, by giving the right steer, supporting the programme, and influencing a change at the cultural level. The DPDP Act influence the entire data management process. Hence, the board must oversee the privacy programme's implementation, governance, and improvement to achieve success.

From ensuring that regulatory obligations are met and industry standards are followed, to fostering a culture of privacy by design and awareness-building initiatives, boards are going to play a pivotal role in steering enterprises towards adapting to the changing data privacy regulatory landscape.

This publication, "The DPDP Act and enterprises in India: Privacy for the board," provides a comprehensive view of the board's role in navigating the DPDP Act. It deals with the provisions of the new law and its impact on enterprises, while providing board members with expert insights on how to approach the operationalisation of the DPDP Act. It also contains a ready reckoner for board members to understand the key questions they must tackle to ensure compliance with the new law.

Executive summary

The 21st century is characterised by unprecedented digital transformation. India is also experiencing rapid digitisation. In the past few years, government-led digital initiatives have made it convenient for citizens to access public services. In contrast, the innovation from the private sector has made customised experiences accessible to consumers. Digital growth has led to an increase in data breaches and misuse of personal information, which has raised concerns over compromised data privacy.

Enterprises acknowledge that data privacy is important to reflect trust and transparency, preserve brand reputation, avoid financial losses, and reduce the risk of data breaches. Furthermore, as awareness regarding data privacy continues to grow, governments worldwide are establishing regulations that balance individual rights with digital advancement.

Indian policymakers introduced the Digital Personal Data Protection Act, 2023 (DPDP Act), on August 11, 2023, to safeguard the personal data of people in India. This new law places specific obligations on enterprises that collect and process personal data to offer consumers goods and services. The DPDP Act also includes provisions to impose penalties in case of non-compliance.

Given the Act's provisions, the expectation from the board is to understand data privacy to develop a top-down approach to guide compliance and foster a culture where privacy is a strategic imperative.

Currently, boards have the following common questions regarding the new law:

1. What kind of material impact does the law have on the enterprise?
2. What governance structure do we have to ensure proper implementation and accountability?
3. What kind of escalation matrix do we have?
4. What is the level of awareness within the enterprise? Do enterprise leaders and the management fully understand the implications of the law?
5. What measures do we need to drive data privacy as part of the culture?
6. What is the proposed plan for mitigating the risks?
7. How does the law impact third-party data sharing?
8. What kind of monitoring mechanisms do we have in place to check for adherence to the law?
9. What is our plan and roadmap to look beyond compliance, and how can the privacy factor enhance trust among customers and other stakeholders?

This publication highlights the provisions of the DPDP Act and how it will impact enterprises in India. Through this publication, we provide insights into how the board can navigate the DPDP Act and the evolving data privacy landscape.

The publication highlights the following:

Chapter 1

From shadows to spotlight to the impending risks: Growing importance of data privacy

This chapter explores the significance of data privacy in today's digital age, highlighting its role in safeguarding individual rights, fostering consumer trust, and mitigating risks associated with data. It also introduces the importance of boards as key change-makers in designing tomorrow's enterprises.

Chapter 2

Deciphering India's data dependence: Navigating privacy amidst digital transformation

India's rapid digitisation has translated into an increasing dependence on data to provide services and experiences. This chapter examines the relevance of data privacy in India and highlights recent developments that have strengthened the idea of privacy.

Chapter 3

Regulatory ripples: Global laws demand attention to data protection and privacy

This chapter examines the key developments and trends in data privacy and protection regulations in major geographies, such as the US, Europe, and Singapore. Additionally, the chapter highlights mandates by Indian regulatory bodies to guide data privacy.

Chapter 4

Demystifying India's data protection law: The DPDP Act

This chapter is an in-depth analysis of the DPDP Act and describes the provisions, scope, key terms, and impact on the enterprise and the board.

Chapter 5

Top imperatives for the board

This chapter provides an overview of the board's responsibilities and obligations in ensuring compliance with the DPDP Act and how they can advocate for increasing the enterprise's privacy quotient.

Chapter 6

Ready reckoner

This chapter contains an easy-to-refer privacy-specific reckoner and questions that boards can consider across the DPDPA implementation journey.

Chapter 7

The future of privacy for the board

This chapter contains the concluding takeaways for boards to stay aware and vigilant and steer the enterprise towards the future of data and privacy.

Chapter 1: From shadows to risks to opportunities: Growing importance of data privacy

In today's digital world, the simple act of uploading a picture on your social media leads to the creation of an extremely valuable commodity—personal data. The phrase "data is the new oil" captures the importance of personal data as a driver for profitability and personalised service provisioning. This reliance on personal data reflects data security, privacy, and legal implications that enterprises must tackle in a structured and harmonised manner.

While personal data can contribute to overall enterprise growth, it has raised concerns regarding data privacy. The increase in cyber threats and misuse of personal data has led to a surge in public awareness regarding individual data rights. Regulators worldwide have created laws governing personal data to safeguard the individual rights of their citizens, such as the General Data Protection Regulation (GDPR) in Europe and the DPDP Act 2023 in India.

Enterprises are increasingly acknowledging the pivotal role that data privacy plays in maintaining consumer trust and brand reputation, along with protection against financial losses and regulatory penalties. Boards are now embracing data privacy as a strategic imperative rather than a simple matter of compliance.

Therefore, a top-down approach is required from the board to create a culture of data privacy, governance and an oversight mechanism that can strategically address rising privacy risks and compliance requirements.

According to the WEF Global Cybersecurity Outlook 2024,[1] 93 percent of respondents who consider their enterprises to be leaders and innovators in cyber resilience trust their CEO to speak externally about their cyber risk, and 60% of executives agree that cyber and privacy regulations effectively reduce risk in their enterprise's ecosystem.

According to a Deloitte report, 61 percent of smartphone users worry about data security and privacy on their phones, and 62 percent of smart home users worry about the same on their smart home devices, respectively.[2]

According to the Cisco 2024 Data Privacy Benchmark Study, 98 percent of enterprises report privacy metrics to their board of directors.[3]

[1] https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf
[2] https://www2.deloitte.com/xe/en/insights/industry/telecommunications/connectivity-mobile-trends-survey/2023/data-privacy-and-security.html
[3] https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2024.pdf

Chapter 2: Deciphering India's data dependence: Navigating privacy amidst digital transformation

The active internet base in India is expected to grow to 900 million by 2025. As a result, India's digital landscape has undergone a seismic shift in recent years, fueled by rapid technological advancements, widespread internet penetration, and government-led initiatives such as Digital India.

The public sector created its digital public infrastructure (DPI), known as India Stack. It comprises unique digital identification, a payments system, and a data exchange layer. This has enabled the government to make various services available to citizens digitally, ensuring convenience and speed.

According to the DPI Nasscom Report, by 2030, India's digital public infrastructure will add between 2.9 and 4.2 percent economic value.[4]

Government-led initiatives such as Aadhaar, DigiLocker, and Unified Payments Interface (UPI) have been instrumental in positioning India as a global leader in inclusive digitisation that considers last-mile connectivity. They have also been instrumental in stimulating innovation in the private space.

Companies are innovating to provide consumers with diverse services on the private sector front. People can use digital platforms for many things, such as opening a bank account, taking medical consultations online, buying insurance, and even booking movie tickets. The falling cost of mobile data ensures an ever-growing increase in the number of consumers who can avail internet services with a single swipe.

Initiatives by the government, innovation from the private sector, and a growing number of internet users have led to rapid digitisation in India. Personal data is being used to avail not only public services but also to attain unique offerings and experiences from private enterprises. The impending awareness around data privacy has grown exponentially as people disclose their data for specific services and experiences.

This reflects in the 2017 landmark judgement that the Supreme Court delivered in the *Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors.* The judgement declared privacy as a fundamental right, protected under Article 21 of the Indian Constitution pertaining to the Right to Life and Liberty.

Consumers are becoming more vigilant about how enterprises use their personal data. For example, according to the Deloitte Global Automotive Consumer Study (2020),[5] 69 percent Indian customers are concerned with the security of data shared with connected vehicles.

Case study: At the beginning of 2024, the Reserve Bank of India imposed business restrictions on the payments bank of a famous fintech company in India. One of the key issues the regulatory body has taken up is the company's non-compliance, which left the bank's customers at risk of data breaches and fraud.

[4] https://community.nasscom.in/communities/digital-transformation/nasscom-arthur-d-little-indias-digital-public-infrastructure

[5] https://www2.deloitte.com/content/dam/Deloitte/us/Documents/manufacturing/us-2020-global-automotive-consumer-study-global-focus-countries.pdf

Chapter 3: Regulatory ripples: Global laws demand attention to data protection and privacy

Governments across the globe acknowledge that digitisation may come at the risk of compromising individual data privacy rights. Laws have been developed across jurisdictions to balance individual rights with economic progress through technological innovation.

Aspect	GDPR (EU)	CCPA (California, USA)	PDPA (Singapore)
Applicability	General Data Protection Regulation (GDPR) aims to safeguard the personal data of people in the European Union. It governs enterprises operating within and outside the EU that offer goods or services to individuals located in the EU or monitor their behaviour. GDPR protects personal data in digital and physical formats.	California Privacy Rights Act (CPRA) is applicable to personal data processing in digital and physical formats related to California residents, and collected by enterprises based out of California, or are doing enterprise in California with an annual revenue above $25 million or is processing personal data of more than 50,000 residents or acquires 50 percent of their revenue from selling data.	The Personal Data Protection Act (PDPA) covers personal data stored in digital and non-electronic formats.
Grounds for processing personal data	Enterprises may rely on grounds such as performance of a contract, legitimate enterprise interest, and consent to process personal data provided it is freely given, specific, informed, and unambiguous. A privacy notice/policy should be provided to individuals on or prior to data processing.	Consent and legitimate enterprise interest are primary grounds for processing personal data. A privacy notice is to be provided to individuals, mandatorily including a “do-not-sell-or-share my information” link for individuals to opt-out of such data processing activity.	Consent is the primary ground for processing personal data, and a privacy notice is to be provided on or prior to collecting such data.
Data breach notification	Once identified, personal data breaches are to be reported to the Data Protection Authority and, in select cases, to the impacted individuals within 72 hours.	At the earliest, report the data breach to the Attorney General’s office and the residents if impacted individuals are more than 500.	Individuals and Data Protection Commission are to be notified no later than 72 hours.
Penalties	€10 million or 2 percent of the company’s global annual turnover, whichever is higher, or €20 million or 4 percent of the company’s global annual turnover, whichever is higher.	Injunction and liable for a civil penalty of not more than US$2,500 for each violation or US$7,500 for each intentional violation.	Financial penalty not exceeding SGD 1 million or 10 percent of annual gross turnover in Singapore (if the annual turnover exceeds SGD 10 million), whichever is higher.

Case study: In 2023, a US-based judge from Delaware refused to dismiss a lawsuit against a social media company's founder and former directors. They allegedly ignored privacy violations and now face the claims in court.

Apart from specific laws such as the DPDP Act in India, guidelines implemented by the regulatory bodies promote good governance and enterprise reporting with regard to data privacy:

Securities Exchange Board of India (SEBI), the regulatory body for securities markets in India, designed the Business Responsibility and Sustainability Report (BRSR) about environmental, social and governance (ESG) reporting. Coming into effect in 2023, one of the disclosures required are the details of cybersecurity and data privacy policies.

The Reserve Bank of India (RBI) released a circular mandating banks to ensure the protection of customer data and for the senior leadership team and board of directors to participate in awareness training sessions aimed at acquainting them with cybersecurity concepts.

Shefali Goradia, Chairperson, Deloitte for South Asia said, “Responsible use of data by an enterprise requires a proactive and strategic approach, and such initiatives are strengthened when there is support from the board. With the DPDP Act, data privacy considerations have become critical across all operations within an enterprise. Hence, the role of board becomes instrumental in redefining the enterprise culture and ethos towards responsible handling of data. This not only helps adhere to regulatory requirements, but also creates an opportunity to build stakeholder trust in this digital era.”

Chapter 4: Demystifying India's data protection law: The DPDP Act 2023

The recently enacted DPDP Act 2023 is a significant move to resolve growing privacy issues. The scope of the new law includes not only the protection of the right to privacy but also promotes enterprises adhering to responsible data management practices.

Applicability	The Act is applicable to data collection occurring within the borders of India, regardless of whether the data is initially gathered in non-digital form and later converted to digital form. Moreover, the Act also covers processing digital personal data outside of India's borders if it is related to any activity that involves providing products or services to Indians living in the country.
Key terms	• "Data Fiduciary " is any person who decides the purpose and the means of processing personal data. • "Data Principal" is the individual to whom the personal data belongs. • "Data Processor" is any person who processes personal data on behalf of the Data Fiduciary. • "Significant Data Fiduciary" is an enterprise that gets notified as Significant Data Fiduciary by the Central Government based on relevant factors such as: a. the volume and sensitivity of personal data processed b. risk to the rights of the Data Principal c. potential impact on the sovereignty and integrity of India d. risk to electoral democracy e. security of the State f. public order
Key provisions	• **Purpose limitation** DPDPA section–5(2)(i), 6(1), 7(a): Enterprises must ensure that their purposes are "specified, explicit and legitimate" • **Security and confidentiality** DPDPA section–8(4): Enterprises shall put in place organisational and technological measures to protect the security and confidentiality of personal data. • **Notice** DPDPA section–5: Enterprises shall provide the data principal with information such as purpose, rights, and procedure to make a complaint. Information should be in clear, easily understandable and in the local/regional language, if required. • **Consent** DPDPA section–6: Enterprises shall get free, specific, unambiguous consent for processing personal data and explicit consent in case of sensitive personal information. • **Data minimisation** DPDPA section–7: Enterprises shall be vigilant about data minimisation and data collection, which are necessary for processing. • **Transfer of data to third parties** DPDPA section–8: Enterprises shall transmit personal data to data processors only with the individual's consent, valid contract between the parties, etc. • **Rights of Data Principals** DPDPA section–11 to 14: Enterprises shall facilitate individual's control over their data by exercising their rights.

Penalties for non-compliance	• Failure to prevent a personal data breach: Up to INR 250 crore. • Failure to notify the breach to the board and data principals: Up to INR 200 crore. • Non-fulfilment of obligations while processing children's data: Up to INR 200 crore. • Non-fulfilment of obligations by a Significant Data Fiduciary: Up to INR 150 crore. • Breach of any voluntary undertaking given to the board: Penalty up to the extent applicable for the breach. • Miscellaneous non-compliance with provisions of the Act: Up to INR 50 crore.
Requisites for Significant Data Fiduciaries	The Act specifies the following obligations for a Significant Data Fiduciary: • Appointing a Data Protection Officer • Appointing an independent data auditor • Initiation of the following measures: – Conducting periodic data protection impact assessments – Regular audits

Implication on enterprise

Enterprise models and operating models will need to be revisited to enable privacy. The following revisions can achieve that:

- Being privacy aware is no longer an option. A culture of privacy will need to be established and sustained.
- Compelling the need to collect and process personal data can't be an afterthought anymore.
- Enterprise development/marketing/digital marketing methods will need to change to become privacy compliant.
- Product development teams must be sensitised and trained on secure coding practices and manage databases, repositories, and storage in a privacy-compliant manner.
- Internal functions, such as legal and HR, will have to upgrade their ways of working, keeping the requirements of the DPDP Act in mind.
- Vendors, visitors, employees, and other stakeholders will need to be evaluated as data principals.
- All third-party engagements must be revisited to ensure that the right processes and controls are in place to handle data safely and responsibly throughout the data life cycle.

Relevancy and impact on board and CXOs

- Board: Ensuring assimilation of the ethos of data responsibility under the umbrella of good corporate governance and stakeholder trust and enabling top-down assimilation, better oversight, and trust-building.
- CEO: Giving the mandate, strategic enterprise alignment, and rigour in implementation.
- CFO: Managing compliance cost and capacity building at the enterprise level. Compliance action plan and propagating privacy-as-a-culture at the functional level.
- COO: Managing compliance across internal functions and throughout the supply chain.
- CHRO: Prioritise responsible data handling for employee and contractual staff across initiatives.
- CMO: Protecting customer data and reimagining the data-driven customer acquisition and retention strategy.
- CTO: Embedding data privacy and protection into the technology stack.
- DPO/Legal: Playing a critical role in deciphering the legislation and revisiting various vendor and partner contracts.
- CISO: Introducing policies, procedures, and controls for privacy and data protection.

"Boards of companies that care about corporate governance are very mindful of the Act. They want to know what to do, how to do, and when to do. Companies that handle a very big volume of data, such as those from the banking sector, will probably get categorised as significant data fiduciaries by the government as per the provisions of the DPDP Act. They understand that they will be held responsible, directly, or indirectly. Hence, they're looking at enhancing their understanding of the role and responsibilities of a DPO and how he/she will report to the board. Boards are mindful of huge pecuniary liability and also the serious reputational issues arising out of any such claim. Today, the stakeholders have a zero-tolerance zone for non-compliances, which adds to the fiduciary responsibility of the boards." (Rajesh Narain Gupta, a seasoned lawyer, serves as an independent director on the boards of multiple companies)

Chapter 5: Top imperatives for the board

The board will play a pivotal role in ensuring compliance with the DPDP Act systematically, balancing the enterprise objectives with key compliance focus areas by taking the following privacy-first approach:

Self-Awareness: The board must familiarise themselves with regulatory obligations to gain a comprehensive insight into the specific requirements and obligations imposed on enterprises regarding data privacy. Additionally, boards must apprise themselves of evolving industry standards to enhance their awareness of emerging trends and risks.

Governance (enterprise, culture, and people): The board needs to drive the culture of transformation and embed data protection and privacy through knowledge sharing, training, and awareness. Further, the awareness levels of employees across enterprise functions should be tested for adherence to privacy policy and procedures, and applicable privacy laws.

Enterprise transformation: As part of enterprise transformation, board members should understand and overcome the data concerns regarding enterprise processes and enable enterprises to generate value from data while taking appropriate care of privacy principles. The board should ensure that the enterprise considers privacy not only as a compliance issue but also by identifying the need to operationalise privacy measures and processes, leveraging technology and automation.

Risk management: The board should consider integrating data protection and privacy as part of its risk function and implement appropriate controls to manage enterprise risk and increase enterprise resilience.

> "There must be proper documentation of the permission requested before processing of data. Ensure that there is evidence of the fact that your enterprise is requesting consent as per the provisions of the DPDP Act." (Shailesh Haribhakti, a certified internal auditor, financial planner and fraud examiner, holds independent directorships with companies)

Third-party risk management: Administrative and technical measures should be implemented to monitor and manage third parties in processing personal data to enhance customers' experience while meeting privacy expectations. The board should consider sensitising the procurement function to give due weightage to privacy obligations when onboarding a supplier and mandate processes to maintain transparency with consumers regarding the privacy maturity of the suppliers handling their personal data.

Proactive compliance: The boards can guide the privacy office and stakeholders across enterprise lines to take the following proactive steps to meet compliance objectives:

01 Commit to informed consent and not retaining personal data longer than the period required per lawful basis.

02 Maintaining a records of processing activities and having visibility over the types of personal data processed across its lifecycle.

03 Transferring personal data securely outside of India per provisions of the DPDP Act.

04 Asking for personal information is reasonably necessary for intended purposes, emphasizing on data transparency and trust while collecting data.

05 Adopting privacy by design approach and deploying strong security controls at all points of data collection, transfer, use, and storage.

06 Educating employees on how to handle personal data securely, reporting data breaches timely, and addressing data subject rights per the DPDP Act.

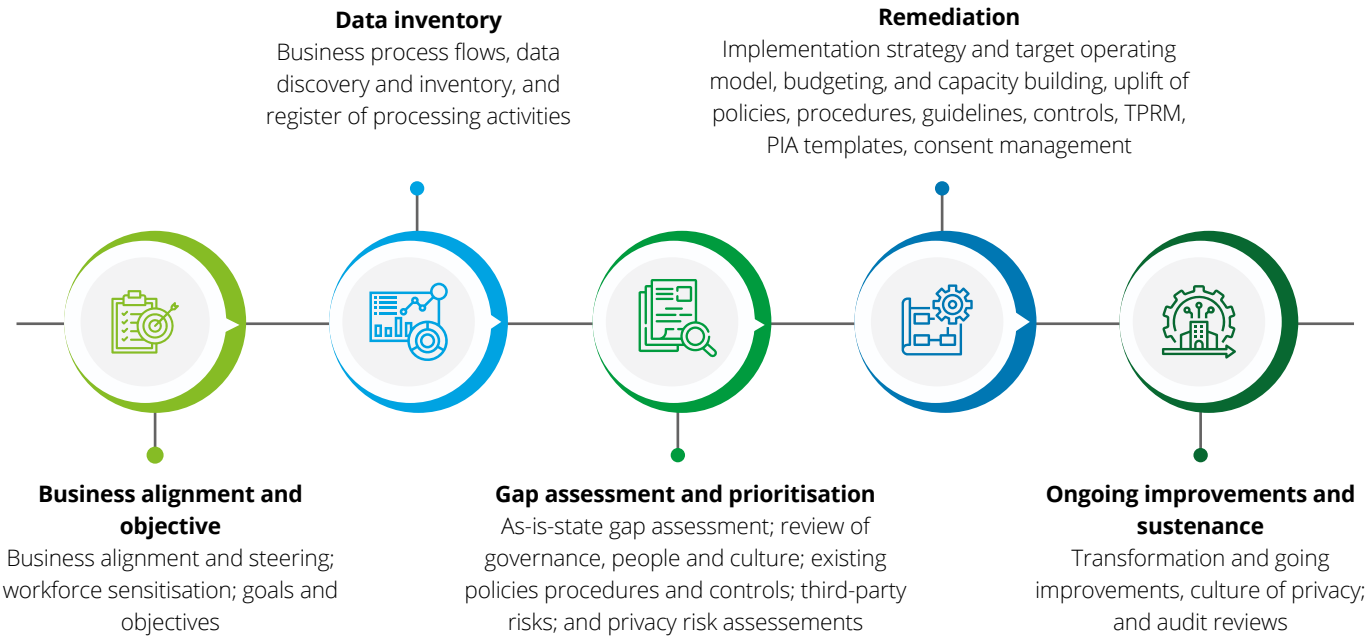
"Currently, the boards are concerned with three primary aspects when it comes to implementing the provisions of the DPDP Act. The first aspect is creating a data privacy policy for their enterprise. The second is understanding who within their enterprise structure will be responsible for the implementation of the new law and monitoring adherence to its particulars. Thirdly, various boards are working towards how to conduct training in a manner where each employee will be sensitised to the principles of data privacy and understand the DPDP Act better." (Rajesh Narain Gupta, a seasoned lawyer, serves as an independent director on the boards of multiple companies)

"When creating a data privacy framework for the enterprise, an escalation matrix must be provided. It will flag areas for the board which require escalation. A risk committee must be formed to track the metrics associated with the compliance of the DPDP Act in real time. Members of this committee can particularly focus on near misses to understand the gap that needs to be filled in their framework. Moreover, the committee should meet with the board twice a year to apprise members of its ongoing initiatives and future plans." (Shailesh Haribhakti, a certified internal auditor, financial planner and fraud examiner, holds independent directorships with companies)

"The board can consider a compliance tool which will monitor the status of compliance and aid in the oversight of the implementation of the DPDP Act. Moreover, the executives must inform the board about the effectiveness of the compliance initiatives. Additionally, as technology-related regulations come into existence, there also is a need and a demand for professionals with a tech background to join the enterprise. Their expertise will go a long way in understanding how to implement the new law in a sound manner." (R Sankaraiah, a seasoned Chartered Accountant, has held the position of director across multiple different boards)

Chapter 6: Ready reckoner

As the steward of an enterprise, the board's role in ensuring robust data privacy practices has never been more important. To begin, it is important to understand the key steps and activities involved (at an enterprise level) in operationalising the DPDP Act.



Aligned with these steps towards privacy readiness, the following ready reckoner provides key questions designed to equip the board to ask pertinent questions at each stage to make informed decisions, mitigate risks, and comply with the DPDP Act:

Process/Step	Target objective	Considerations for the board (Key questions to ask)
Business alignment and objective	• **Steering committee:** Establishing a steering committee to oversee the enterprise's data privacy strategy. The committee will be responsible for setting strategic direction, allocating resources, and structuring alignment with enterprise objectives. • **Workforce sensitisation:** Imparting first-level awareness among employees and key stakeholders through training programmes, awareness campaigns, and interactive workshops to strengthen their understanding of data privacy principles, policies, and best practices. • **Goals and objectives:** Establishing a desired state per the law's applicability and overall data and privacy goals, setting timelines and defining KPIs.	• Has a dedicated steering committee for data privacy governance been established? • Does it have representation from across enterprise functions? • Do we have a proper governance structure which provides for accountability? • Is every functional leader sensitised on DPDP Act and its implication for his/her function? • What is the plan on sensitising the workforce and keeping them privacy aware as an ongoing exercise? How are you measuring the effectiveness? Are there any gaps and how are you planning to address the gaps? • What mechanisms are in place for regular monitoring and review of progress towards achieving data privacy objectives in general, and the DPDP Act compliance in particular?

Process/Step	Target objective	Considerations for the board (Key questions to ask)
Data inventory	• **Enterprise process flows:** Mapping out enterprise's processes to identify data flows, including documenting how data is collected, processed, stored, and transmitted throughout the enterprise's systems, applications, including the third parties. • **Data discovery and inventory:** Identifying and cataloguing the enterprise's data assets. It involves data discovery exercises for the purpose of locating sensitive data, categorising data types, and creating an inventory of those data assets. • **Record of processing activities:** Maintaining a register or inventory of data processing activities carried out by the enterprise, including the details of data transfers to third parties.	• How assertive are we about "Know Your Data (KYD)"? Are we confident about personal data we have, its sources, its end of lifecycle, its storage locations, its master vs duplicate copies etc.? • How do we ensure that the record of processing activities is regularly reviewed to reflect the changes in regulatory requirements or data processing practices? • Have we identified key touchpoints within each enterprise process where personal data is accessed, shared or transferred? • Have we revisited our enterprise processes to integrate privacy considerations (as per the law)? • Is there a common understanding and nomenclature being followed to identify and categorise personal data throughout the enterprise, across systems and applications? • Are data discovery efforts inclusive of both structured and unstructured data sources, including legacy systems and third-party platforms? If not, what is being done towards that end? • How is it ensured that all processing activities are documented in accordance with the requirements of the DPDP Act, including data minimisation and purpose limitation principles? • What safeguards are in place to protect data subjects' rights under the DPDP Act?
Gap assessment and prioritisation	• **As-is-state gap assessment:** Assessing the current data privacy practices and identifying gaps or deficiencies in regulatory requirements and industry standards. • **Review of governance, people, and culture:** Evaluate the existing policies, procedures, and controls, including their effectiveness in promoting a culture of privacy. • **Existing procedures and controls:** Conduct a thorough analysis of the enforcement of existing procedures, assessing the adequacy of technical and administrative control to protect data. • **Third-party risks:** Evaluate risks posed by third-party vendors, suppliers, and service providers who have access to the enterprise's data, including assessing third-party contracts, conducting due diligence on third-party security practices, and implementing controls to mitigate third-party risks. • **Privacy risk assessments:** Conduct privacy risk assessments to identify, analyse, and prioritise privacy risks within the enterprise.	• Has a risk identification and mitigation plan with defined roles and responsibilities and mitigation timelines been developed? • Is there a remediation action plan in place, specifically to mitigate the risks of high or critical severity? • Is there a process to track compliance for mandatory privacy training undertaken by the employees? In case of non-compliance, what is the remediation plan to ensure full compliance with such training? • Does the enterprise collect and/or process personal data of children and for person(s) with disability? • Is there a remediation timeline in place to tackle the gaps identified? • What methodologies and criteria are used to assess the likelihood and impact of privacy risks on the enterprise? • Is the board aware about the material impact on the enterprise of not complying with the DPDP Act? • Does the grievance redressal in place currently reflect the requirements of the DPDP Act?

Process/Step	Target objective	Considerations for the board (Key questions to ask)
Remediation (at strategic and operational level)	• **Implementation strategy and target operating model:** Create an implementation strategy and target operating model to address gaps and deficiencies identified through gap assessments. • **Budgeting:** Define a budget and allocate financial resources to implement data privacy remediation efforts. • **Capacity building:** Improve the enterprise's capacity to effectively manage data privacy risks and compliance requirements. • **Operational implementation:** – Detailed review and uplift of privacy policies, standards, guidelines, and procedures – Implement consent management and Data Principal rights management through processes, tools, and grievance redressal mechanisms – Data security controls such as Identity and Access Management and privacy-enabling technologies – Third-party risk management with revision of legal contracts – Breach handling processes, such as detect and respond, crisis management, forensics, and cyber insurance coverage – Privacy-by-design/by-default	• How can we prioritise the adoption of "privacy by design" and "data minimisation" principles? • How do we monitor and evaluate third-party performance and adherence to data privacy standards over time? • How is the identity of the guardian confirmed when taking consent to process the personal data of a child, or person with disability? • In case of a data breach, do we have a crisis management and communication plan in place? • Does the enterprise have a privacy control framework in place that factors in privacy principles such as transparency, consent management, redressal of privacy rights, and data breach management? • Have the relevant budgetary allocations for privacy programme development and maintenance, investments in privacy-enhancing technologies, and staffing of skilled privacy professionals been used to their full impact? • Do we have a centralised consent management framework? • Are the policy procedures governing privacy-related obligations uplifted and customised per changes in legal requirements and technology, and impact on enterprise? • Have changes been made to vendor contracts to reflect the requirements of the DPDP Act? • How are we addressing the conflicts between the provisions of the DPDP Act and other regulatory requirements?
Ongoing improvements and sustenance	• **Transformation and ongoing improvements:** Enhance overall data privacy posture over time through continuous transformation and improvements using emerging best practices. • **Culture of privacy:** Pave the way for a strong privacy-oriented culture, which can be achieved by raising employee awareness. • **Audit reviews:** Ensure compliance with data privacy regulations by conducting regular audits.	• Are there ongoing efforts to improve technology to comply with the requirements of the DPDP Act? • Are playbooks created to make employees aware about securely handling personal data across its life cycle? • Are changes being made to the Code of Conduct document to include processes for reporting instances of violation of the DPDP Act? • How is it ensured that audit recommendations are promptly addressed, and corrective actions are implemented? • Are we investing in technologies to enhance privacy compliance?

"A board member should start by identifying who is responsible for ensuring compliance within the organisation. Next, they should inquire about the organisation's level of compliance and any existing gaps that may be known, leading to asking about the organisation's privacy plans and their ability to execute them in terms of people, process and technology. It is crucial to understand the risks of non-compliance with regulations and how the organisation compares to its peers in the industry." (Ashish Surti, Chief Digital and Information Officer for a leading multinational telecommunications company)

Chapter 7: The future of privacy for the board

Boards are grappling with risks outside their traditional remit. Data privacy concerns are intertwined with an enterprise's growth journey, impacting enterprise continuity, infrastructural and network security, and consumer trust. Moreover, new privacy regulations continue to emerge worldwide, further contributing to complex requirements to an already complicated mix of regulatory and legal compliance landscape dealt with by the board. For building a resilient privacy program, it is important to maintain data privacy and security vigilance, and methodically enable the Privacy Office. Board members should focus on specific action areas.

"The DPDP Act has pushed board members to ask the management questions on preparedness. Towards that end, specific committees might be formed and tasked with the responsibility to understand the impact of the new law. What needs to happen is raising awareness among the board members in a sustained way which will aid in understanding the risks for their organisation. Currently, the boards are broadly aware of the provisions of the Act but understanding it at a granular level will help determine the points of failure relevant to them." (Priya Subbaraman, a seasoned regulatory and compliance professional, serves as a director across different boards)

"In my experience, boards can approach the implementation of data privacy regulation through three critical steps. The board must provide visible sponsorship. Data privacy has to trickle down the whole organisation. For that, you need a champion at the board level who can provide that. Secondly, particularly in the implementation phase, the board can encourage collaboration between different teams to ensure everyone is on the same page regarding what the new law means for the organisation as a whole. Thirdly, the board can take an active initiative to embed the concept of privacy as a shared responsibility across the organisation. It goes a long way in sustaining the data privacy programme." (Jitender Arora, Partner, Deloitte UK)

Five key takeaways that the board should focus on:

Integrated risk management: Data privacy risk assessment and mitigation strategy should be treated as an enterprise-wide risk and compliance activity. This would include strategic staffing, comprising professionals fluent in law, technology, and enterprise. Hence, privacy professionals would be at a good vantage point to work across the enterprise lines and translate policies into practice. Further, privacy risks should be delineated across enterprise lines, and well-defined roles and responsibilities should be codified to ensure that the enterprise can factor in and manage new privacy regulations or privacy risk reporting efficiently.

Resilient oversight: Considering that privacy is a relatively young function in an enterprise, balancing adhering to multi-faceted compliance activities and staffing could pose a challenge. Therefore, the board should consider developing a reporting structure and affixing a reporting frequency that helps their enterprise reach privacy maturity sustainably and at scale. At the same time, they dabble with striking the said "balance". Hence, external professionals may also be leveraged to assist with critical matters like data discovery, impact assessments, and privacy incident remediation, as they have access to technologies and cross-disciplinary skills and can offer insights and reports on how your peer companies are managing similar issues.

Cultural considerations: A top-down approach is key to building a privacy-enabled enterprise rather than just a privacy-compliant enterprise, per which employees across enterprise lines imbibe the importance of data privacy and protection through regular communication and training led by senior management and board members. To this effect, periodic role-based training that tests the knowledge of the employees on secure data handling is a good starting point to embed the culture of privacy, supplemented by awareness sessions from industry experts.

Continuous monitoring: The board should be cognizant of the value of continuous monitoring and reporting as it plays a key role in achieving a healthy compliance posture. The goal is to achieve seamless and continuous monitoring and reporting that aligns with the established privacy risk policy and privacy notices and enables coordination and cooperation channels with the data protection authorities. The privacy office should have monthly check-ins to report non-adherence to privacy obligations and escalate risks and control issues.

Strategic investments: As reliance on data to meet enterprise objectives is only rising, privacy-enhancing technologies and computation techniques would become a standard for enterprises across industries to automate compliance activities. Therefore, the board should proactively assess the budgetary and technical factors to strategically invest in such techniques from financial and human resource standpoints. Per Gartner, "Unlike common data-at-rest security controls, privacy-enhancing computation (PEC) protects data in use. As a result, enterprises can implement data processing and analytics that were previously impossible because of privacy or security concerns. Gartner predicts that by 2025, 60 percent of large enterprises will use at least one PEC technique in analytics, enterprise intelligence and/or cloud computing."

Boards must go beyond examining data privacy as a regulatory compliance issue and focus on creating a culture where privacy principles are reflected in day-to-day operations, contributing to an overall trust in the ecosystem.

Confederation of Indian Industry

The Confederation of Indian Industry (CII) works to create and sustain an environment conducive to the development of India, partnering Industry, Government and civil society, through advisory and consultative processes.

For more than 125 years, CII has been engaged in shaping India's development journey and works proactively on transforming Indian Industry's engagement in national development. With its extensive network across the country and the world, CII serves as a reference point for Indian industry and the international business community.

As India strategizes for the next 25 years to India@100, Indian industry must scale the competitiveness ladder to drive growth. CII, with the Theme for 2023-24 as 'Towards a Competitive and Sustainable India@100: Growth, Livelihood, Globalisation, Building Trust' has prioritized 6 action themes that will catalyze the journey of the country towards the vision of India@100.

Confederation of Indian Industry
The Mantosh Sondhi Centre, 23, Institutional Area, Lodi Road, New Delhi – 110 003 (India)
T: 91 11 45771000; E: info@cii.in • W: www.cii.in

cii.in/facebook cii.in/twitter cii.in/linkedin cii.in/youtube

Reach us via CII Membership Helpline Number: 1800-103-1244

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte enterprise"). DTTL (also referred to as "Deloitte Global") and its member firms and related entities are legally separate and independent entities which cannot obligate or bind each other regarding third parties. DTTL and each DTTL member firm and related entity is liable only for its acts and omissions and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more. All the facts and figures that talk to our size and diversity and years of experiences, as notable and important as they may be, are secondary to the most accurate measure of Deloitte: the impact we make in the world. So, when people ask, "What's different about Deloitte?" the answer resides in the many specific examples of where we have helped Deloitte member firm clients, our people, and sections of society to achieve remarkable goals, solve complex problems or make meaningful progress. Our beliefs, behaviours, and fundamental sense of purpose underpin all we do. Deloitte Globally has grown in scale and diversity—more than 415,000 people in 150 countries, providing multidisciplinary services, yet our shared culture remains the same.

Connect with us

Deloitte

Anthony Crasto
President, Risk Advisory, Deloitte India
acrasto@deloitte.com

Abhijit Katkar
Partner, Risk Advisory
Deloitte India
akatkar@deloitte.com

Tarun Kaura
Leader – Cyber Leader, Risk Advisory
Deloitte India
tkaura@deloitte.com

Manish Sehgal
Partner, Risk Advisory
Deloitte India
masehgal@deloitte.com

CII

Vikkas Mohan
Principal Adviser, CII
vikkas.mohan@cii.in

Chitra Mittal
Senior Director, CII
chitra.mittal@cii.in

Contributors

Deloitte

Manishree Bhattacharya
Grace Bains

CII

Chetna Agarwal

Acknowledgment

Jayita Mukherjee
Vijaya Lakshmi
Neha Kumari
Swati Manocha

Hunny Gureja, CII

Confederation of Indian Industry

Published by Confederation of Indian Industry (CII), The Mantosh Sondhi Centre; 23, Institutional Area,

Lodi Road, New Delhi 110003, India, Tel: +91 11 45771000; Email: info@cii.in; Web: www.cii.in

Deloitte.