A CFO’s guide to navigating the Digital Personal Data Protection Act, 2023
Transformation of the CFO (Chief Financial Officer) function and the emergence of newer data value chains

From managing P&Ls and payrolls, to driving innovation and spearheading digital transformation in handling financial data, the office of the CFO provides strategic direction to an organisation. The CFO’s purview encompasses the management of financial risks for the organisation - an integral aspect of which entails the responsibility of data processing.

Within an organisation, the CFO’s office is the nerve centre where data flows from various departments as part of operations. The finance function also exchanges data with third parties for functions such as payroll processing, insurance, health and wellness programmes, etc. In addition, the CFO’s office governs major business decisions that might involve the collection of personal information from customers.

The Digital Personal Data Protection (DPDP) Act, 2023

On 11 August 2023, the President of India signed the Digital Personal Data Protection Bill, 2023 into law. The DPDP Act 2023 regulates the processing of digital personal data in a manner that recognises both, the rights of individuals to protect their personal data, and the need for organisations to process personal data, for lawful purposes. The Act’s provisions cover personal data in digital format, including both data that originates digitally, and non-digital data that is subsequently digitised. The provision applies to data processing within and outside India, if it relates to the offering of goods or services to individuals within India.

It should be noted that personal data processed by an individual for personal or domestic purposes, as well as publicly available data, fall outside the scope of this Act.

Key coverage

The Act is aimed at empowering individuals (termed “Data Principals”) to receive information about their personal data, correct, update, or delete their personal data, seek grievance redressal for errors made by Data Fiduciaries, or nominate a third party to act on their behalf.

For enforcement, it necessitates the establishment of the Data Protection Board of India, which will be responsible for identifying non-compliance, investigating complaints of violations and more.

Penalties for non-compliance span multiple categories (up to INR 250 crore per incident for failing to prevent a personal data breach).

The act lays out obligations for “Data Fiduciaries” (any person, including legal entities, who determine the purpose and means of processing personal data). These obligations include providing notices; obtaining due consent to process personal data only for legitimate use; maintaining the accuracy of personal data; protecting personal data; erasing personal data once the purpose is served or when the Data Principal withdraws their consent; obtaining verifiable parental/guardian consent for the personal data of minors or persons with disabilities; immediately notifying breaches; and other related measures.

Click here to read the detailed PoV covering provisions and exceptions of the Act.
Gearing up for the Act – Top five imperatives for a CFO

At the organisation level

1. **Taking the lead in managing the costs of compliance and failure to comply**

   The Act places the responsibility on Data Fiduciaries to comply with the law. It necessitates them to prioritise Data Principal rights and mandates the implementation of appropriate technical and organisational measures to safeguard these rights. The cost of non-compliance may involve penalties of up to:
   - INR 250 Cr in the event of a breach resulting from the absence of reasonable safeguards.
   - INR 200 Cr for failing to notify the Data Protection Board or a Data Principal about a data breach.
   - INR 200 Cr for violations while processing children's personal data.

   It is important to note that these penalties are applicable per event, which implies that the cost of non-compliance could be significantly higher.

   It is imperative for the CFO office to strike a balance between compliance costs and the organisational obligations as Data Fiduciaries. This is essential to mitigate the risks of incurring substantial penalties in case of a failure to comply.

   Creation of a DPDPA corpus fund from the CEO’s office is an important consideration to make additional budgets available and enable smoother implementation across business functions.

2. **Be an important part of the DPDPA cross-functional executive working committee**

   CFOs sit at the heart of this implementation and can contribute by being a part of the executive committee that lays out the compliance action plan. This committee must be chaired by the CEO/COO’s office, with the CISO as a co-chair. The CFO, as part of this committee, can direct the new line of CEO budgeting to the best usage, across the various workstreams of the DPDPA implementation.

3. **Being the champion – spreading awareness, assisting in capacity building, and establishing governance**

   As the custodian of risk management, the CFO bears the responsibility of aiding both function heads and the entire organisation in adapting to the Act. It is important for CFOs to comprehend how the Act alters the way organisations collect and manage personal data, along with the repercussions if mishandled.

   From the corpus fund made available at an organisation level, the CFO should allocate budgets for appointing a data privacy and protection team, to collaborate with security leaders and the management to define the privacy function. This collaboration involves supporting capacity building, facilitating reskilling, spreading awareness, and establishing a governance framework. A Data Protection Officer, DPO, may also need to be appointed, as necessary.

As head of the finance team

4. **Establish a plan of action for financial processes**

   To embark on the journey toward compliance for financial processes, it’s crucial that the CFO brings in guidance and learning from the executive working group. This group has the responsibility to formulate the compliance action plan including consent management, classification, data security, and the implementation of privacy practices for personal data, and the CFO must adequately sensitise his/her function on their roles and responsibilities to support the implementation.

   The CFO can take the lead in organising immersive workshops tailored to the needs of his function, and for the management of financial processes. These workshops can offer scenario-based learning to enhance the implementation of processes and controls, improve crisis management strategies, and explore technology-driven innovations.

5. **Build a culture of privacy**

   The CFO has visibility into all business processes and comprehends the impact of these processes on the organisation’s success. The organisation must reassess these processes and integrate the principle of “privacy by design”, which entails considering privacy implications before making any business decisions. To ensure the effectiveness of this approach, organisations should also raise awareness among all stakeholders within the value chain.

   In a landscape where data breaches and privacy concerns have far-reaching consequences, the CFO’s involvement in the DPDPA Act compliance becomes more important. Beyond the legal aspects, the CFO, being the guardian of the business and an influencer, shoulders an important responsibility to ensure the organisation’s seamless and effective compliance with the DPDPA Act, both from a financial and reputational standpoint. By actively championing DPDPA Act compliance, the CFO reinforces the importance of safeguarding individuals’ privacy rights while also cultivating trust among customers, partners, and other stakeholders.