Grant Thornton

GLOBAL FINTECH FEST

Implications of the DPDP Act 2023 on India's Financial Services Sector

Contents

Foreword

Deepankar Sanwalka
Senior Partner - National Management
Grant Thornton Bharat

The conversation on data is not an option today; it is a necessity. With our digital footprint increasing with every click, online transaction, card swipe, etc., it is imperative that data handling and privacy take centre stage. The new Digital Personal Data Protection Act 2023 (the Act), with its robust framework for data handling and privacy, has set the tone for shaping a secure digital-first ecosystem in India. The Act has set detailed guidelines, applicable across sectors and industries – including the Financial Services sector – to help businesses establish a gold standard for effective handling of personal data.

The financial services sector is one of the most regulated sectors in the country and follows several existing guidance, regulations and frameworks from the Reserve Bank of India (RBI), Securities and Exchange Board of India (SEBI), Insurance Regulatory and Development Authority of India (IRDAI) and other laws like the Information Technology Act, 2000 (IT Act), to ensure effective handling of personal data. However, the exponential growth of the Fintech ecosystem in recent years – India recorded 114 billion digital transactions in FY 2023, according to Statista – has fuelled the need for robust regulatory frameworks to ensure data security, privacy and compliance. To this effect, the new Act, designed to safeguard the privacy and security of personal data in the evolving digital world, is a milestone for the country and the people of India and is a great step towards responsible data handling and protection.

The Act oversees the processing of digital personal data, balancing individuals' rights to safeguard their information with the lawful need for data processing. Obtaining user consent for specific data processing purposes empowers individuals with data ownership. The Act also grants users the right to access, modify, and withdraw consent for their stored data. Our report covers the nuances captured in the Act and sheds light on how it impacts financial services firms, the Fintech ecosystem and their operations.

I believe personal data is sacrosanct and businesses that treat it so, while harnessing and processing this data to gain competitive advantage, will be the ones that will earn consumer trust and loyalty. It is now up to organisations to look at the Digital Personal Data Protection Act 2023 as a business opportunity and create a safe and digital-first #VibrantBharat.

01

Introduction

In an increasingly digital world, the concept "Data is the new oil" aptly captures the value of personal data in contemporary business operations. Personal data, consisting of individual's information ranging from demographic details to behavioural patterns, holds immense potential as a strategic asset for businesses. It drives decision-making, enables personalised services and fuels innovation. Therefore, aided by the digitalisation of the Indian economy and recent technological progress, there is an explosion in the availability of personal data, with businesses processing this data to gain competitive advantage.

The financial ecosystem has also undergone significant transformation in recent years, revolutionising the way financial services are accessed and consumed. While the potential benefits of personal data are significant, the collection, storage, and utilisation of such data have increasingly raised concerns about privacy and security. Unauthorised access, data breaches, and misuse of personal information have become compelling issues, threatening privacy rights of individuals, and fostering mistrust in data practices of businesses. Therefore, there was a compelling need to put in place robust regulatory frameworks to ensure data security, privacy and compliance.

The Data Protection and Digital Privacy Act (DPDPA) of 2023 has consequently emerged as a critical catalyst in enhancing compliance measures. Enacted as a response to the evolving digital landscape, the DPDPA is designed to safeguard the privacy and security of personal data in the digital realm. Its core objectives include empowering individuals with data ownership rights, setting stringent data handling standards and including negative incentives for driving a stronger compliance culture.

Value of personal data in business

Personal data has transformed into a valuable asset that powers various aspects of modern business operations. Companies within the financial services sector leverage personal data for:

Customer insights: This enables firms to develop marketing strategies, product positioning and enhancing customer experience and is a critical component for firms to stay connected and relevant to their customers

Regulatory compliance: Financial services firms are subject to a complex set of regulations and guidelines designed to protect customers, maintain market integrity, and prevent financial crimes; deep understanding of customer through data helps firms to manage these compliance requirements effectively

Risk assessment: Risk transformation is the principal activity undertaken by financial services firms, and relevant data aids risk assessment as well as provide appropriate pricing of risk

Innovation and hyper-personalisation: With the advent of mobile devices as one of the primary channels for delivery of financial services, customer data insights can be used to tailor offerings to individual needs and preferences.

Operational efficiency: Data-driven insights enables firms to take informed decisions, allows for process optimisation, and facilitates efficient resource allocation, leading to cost savings and operational efficiencies

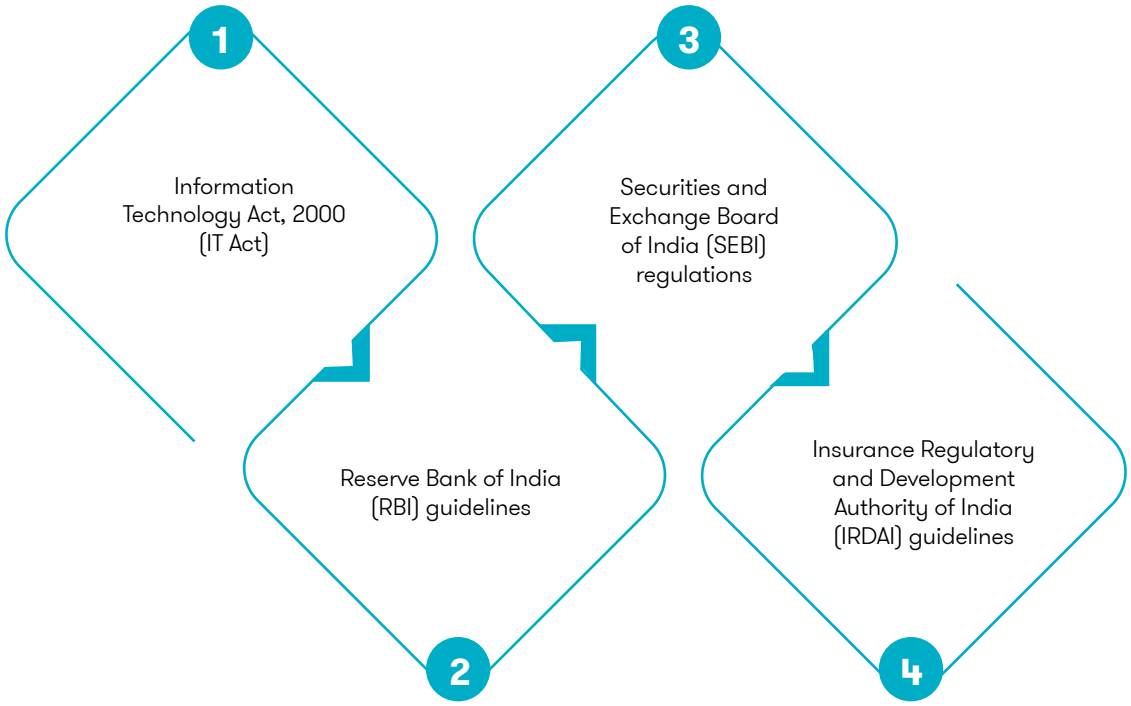
02

Regulatory landscape

The financial services sector is one of the most regulated sectors in India. Regulators, through guidelines on customer protection and data privacy, outsourcing, information security, technology, and cyber risk management, among others, have emphasised many of the aspects that are now codified in the DPDPA 2023.

The extant legislative framework and sectoral guidelines of customer protection and privacy have been built on the principles of fairness, purpose limitation, data minimisation and storage limitation, which also form key components of the DPDPA 2023. However, the DPDPA 2023 goes well beyond the existing acts and regulatory guidelines and keeps the individual's interest at the core of the design of the Act.

Existing regulations, guidelines, and frameworks related to data privacy and security



Furthermore, the sector participants are also a 'Reporting Entity' under the Prevention of Money Laundering Act (PMLA), which mandates the collection and retention of certain data by reporting entities. The intersection of these two Acts will require the financial sector participants to evolve a more nuanced approach towards compliance with the DPDPA 2023 as compared to unregulated entities. Aspects on legal basis for capturing additional data from customer, record retention, archival and disposal, sharing of data with authorities, among others will require extensive deliberation to develop the roadmap for compliance. Given that the sector in general has a long history of complying with strict privacy and data protection rules set by regulators, their approach and detailed procedures towards compliance are likely to be more mature than those of firms in other sectors.

The Act not only empowers individuals to exercise their rights to privacy, but also emphasises on aspects of accuracy, confidentiality, integrity and availability of individual's data, and demands increased accountability from data fiduciaries and data processors covered under it.

03

Key impact areas for financial services

The DPDPA brings transformative effects to various functions within the financial services sector. Here is how it will impact core operational areas:

Regulatory changes

DPDPA 2023 states that Significant Data Fiduciaries will need to be identified and we expect the Financial Services ecosystem to be tagged as "Significant" and thereby have a wide array of responsibilities under the Act. We expect the financial services regulators to adopt the DPDPA and customise it to the sub-sectors that they regulate through appropriate regulatory directions. It will also be worthwhile for the regulators to train their supervisory staff in these new areas for stronger and more robust supervision.

Customer protection is an integral component of regulators' supervisory and regulatory function. Till now, in absence of a legislative framework for customer's data protection and right to privacy, the regulators have issued directions to regulated entities on customer protection and data privacy, which underpinned the principles upon which the DPDPA has been drafted. It is worthwhile to note that in September 2022, while DPDPA was still under development, the Reserve Bank of India (RBI) had to issue specific guidelines on prohibiting Digital Lending Applications (DLA) to access certain mobile phone resources of borrowers, most likely, because it felt that access to such resources violated the principles of fairness, purpose limitation and data minimisation. DPDPA empowers the regulators to further build on their existing initiatives pertaining to customer protection and right to privacy. Under the DPDPA, Data Protection Board (DPB) will be established and tasked with monitoring compliance with the Act, among other things. We anticipate that the sectoral regulators will work closely with the DPB and issue recommendations, guidelines, and frameworks to ensure that financial institutions' data handling practices are in line with DPDPA principles. Key steps that are likely to be taken by the sectoral regulators are as follows.

- **Aligning regulations:** Regulators will review their extant guidelines to ensure that existing financial regulations and data protection laws are aligned with DPDPA requirements to prevent conflicts between financial regulations and DPDPA principles related to data protection and privacy. Significantly, regulatory instructions on "Know Your Customer" (KYC) may undergo certain modifications. The KYC Master Directions, derived from the requirements set out in the Prevention of Money Laundering Act (PMLA), require certain customer data be obtained and retained for offering financial services by the regulated entities (RE). While the guidelines make customer consent mandatory for obtaining customer information, any additional information captured by the REs under its customer acceptance policy will require sound legal basis and should comply with the principle of data minimisation under the DPDPA. The entities will be guided by the regulatory instructions on setting appropriate retention periods for the data collected during AML/KYC processes and customer data should be retained only for as long as necessary to fulfil AML obligations. Regulator may reiterate that while sharing of customer data with relevant authorities for AML purposes is a legitimate interest under DPDPA, it must be ensured that the data shared is proportionate and necessary for the requesting authority. Furthermore, regulators may advise institutions to ensure that customers' rights under DPDPA, such as the right to access their data and rectify inaccuracies, are respected within AML/KYC processes, and encourage institutions to conduct Data Protection Impact Assessments (DPIAs) to assess the potential privacy risks associated with AML/KYC procedures. Other regulatory instructions on customer protection, data privacy, third party due diligence and monitoring, among others, may get reviewed and updated in line with the DPDPA requirements.
- **Promoting awareness and training:** Regulators will focus on promoting awareness about DPDPA among financial institutions to ensure there is appropriate sensitivity and awareness within the ecosystem. Regulators may do so by issuing guidance documents to help REs understand the implications of DPDPA and how to comply with its requirements. These documents may include recommendations on data processing, consent mechanisms, data breach reporting, and more. Furthermore, they may organise workshops, seminars, and training sessions to help REs understand the regulation's requirements and implications. Regulators, along with DPB will collaborate to avoid conflicts and overlaps between financial regulations and data protection laws.
- **Monitoring compliance:** Regulators shall include monitoring the compliance of financial institutions with DPDPA 2023 requirements as part of their supervisory toolkit. Regulatory inspections may be enhanced to include examinations and assessments to ensure financial institutions are appropriately handling customer data and protecting privacy.

Financial services firms deal with large sets of customer information which they require to assess risk and undertake risk transformation activities. While the DPDPA impacts all sectors dealing in customer information, given the existing framework on customer protection and data privacy put in place for the financial services sector regulators, we expect the sector to assimilate and implement the DPDPA requirements more seamlessly as compared to some of the other unregulated sectors.

Risk management

Players in the Banking, financial services and insurance (BFSI) domain will be the data fiduciaries who will be primarily responsible for ensuring compliance to the provisions of the Act from a data protection standpoint. Risk management is fundamental to financial services firms and central to their core function of risk transformation. These institutions leverage diverse customer-related data sources, including alternative data, for risk assessment tied to transactions. Personal data of data principals is leveraged to determine the entity's risk appetite, conduct overall risk assessment, identify potential impacts and ensure adequate management of associated risks. While personal data is not necessarily used at an individual level, the risk management function will have to ensure that consent is available before processing or conducting any analytics on the personal data submitted by data principals.

- **Data and risk management:** Data is leveraged to support precise credit risk pricing, efficient insurance underwriting, and fraud risk evaluation. With the DPDPA, firms must scrutinise collected data, validate legal grounds, and secure specific customer consent. However, potential consent variations could affect risk management efficiency, necessitating preparations and potential pricing adjustments in response to data gaps. As a next step, the risk management functions of financial institutions must conduct a data protection impact assessment with an intention to achieve two primary objectives:
  - To understand the current state of the personal data that is leveraged and critical to the activities conducted by the second line of defence and
  - To prioritise its next steps with respect to the critical data sets for which consent must be sought immediately
- **Enterprise Risk Management:** The Act will formalise the concept of data privacy risks, which was often spoken about but no framework was established for that from an enterprise-wide risk management standpoint. Financial institutions would need to appoint an independent data protection officer (DPO) who shall report to the board of directors and who shall be responsible for management of risks associated with digitised data. The risk management functions would need to set up a framework for periodic monitoring, tracking, and reporting of anomalies identified from a data standpoint. Key Risk Indicators (KRIs) need to be built to ensure that any potential non-adherence to the requirements of the act is highlighted and flagged off periodically to consequently avoid any breach which would invite financial penalties.
- **Sectoral impact:** While each financial institution will face a different set of challenges from a risk management standpoint, insurance companies/brokers will need to heavily invest in identification of data sets/information that is available with their agents and other distributors, which carry customer data freely available in the market. They will need to obtain consent from those data principals who had shared their personal data with their agents or distributors prior to commencement of the Act, i.e., the source of the "publicly available" personal data need to be traced and consent needs to be obtained.

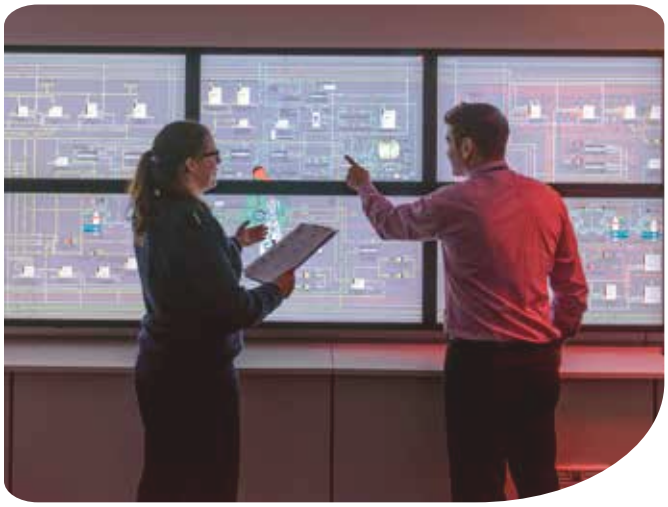
IT and cyber security

DPDPA's strong focus on personal data protection reshapes IT and data safeguarding practices. Financial institutions hold considerable amounts of personally identifiable and sensitive information including financial data, which attract cybercriminals. DPDPA mandates strict compliance checks on data privacy and protection, demanding organisations to relook at investments in advanced threat detection, strong encryption, and regular audits. Implementing these measures helps create an environment safeguarding customer data, preventing unauthorised access, and minimising breach risks.

At a time characterised by swift digital transformation, the merging of IT security and the protection of personal data has gained utmost significance. The DPDPA, with its rigorous directives and responsibilities, magnifies the imperative of aligning robust information technology security practices with the safeguarding of individuals' personal information. We believe that there will be a symbiotic interplay between IT security and the DPDPA, accentuating crucial considerations and strategies for organisations to ensure compliance while reinforcing their digital landscapes against evolving cyber threats.

- **The Landscape of the Act:** The DPDPA embodies a paradigm shift in data governance, advocating for transparency, accountability, and rights of data principals over their data. Financial institutions must understand that effective IT security is not merely a compliance but a strategic imperative to uphold the principles enshrined in the DPDPA. The shift requires moving on the accountability ladder from "owning it up" to "finding new solutions" and "implementing the same" to enhance the current data privacy and security procedures.
- **Increased investments on IT Infrastructure:** Substantial investments in IT security are imperative to augment an organisation's resilience against cyber threats. This will encompass the development and deployment of advanced security protocols, the adoption of cutting-edge cybersecurity technologies, and the recruitment of proficient experts for threat detection, predictive analysis, and automated responses to security incidents. These investments facilitate the expansion of the IT infrastructure, enabling comprehensive controls across every facet of security management, including firewalls, intrusion detection systems, encryption tools, and secure communication platforms.
- **Synergy between IT Security and DPDPA:** IT security forms the bedrock to achieve compliance with the DPDPA. A breach not only jeopardises data but also erodes trust. An integrated approach, where IT security measures come together with the principles of data protection, establishes a holistic and fortified defense against cyber threats. The concept of Continuous Control Monitoring (CCM), prevalent in finance functions of financial institutions, will now extend to IT. CCM involves creating an ongoing control monitoring framework, overseeing controls throughout the data lifecycle management. This framework necessitates constant updates to manage emerging threats, evolving product requirements, and new data security standards. Considering that IT security transcends organisational boundaries, evaluating the data protection practices of third-party vendors and partners becomes pivotal to thwart potential breaches stemming from external sources.
- **Regular Internal and Independent Audits:** Despite significant investments in governance and IT security controls, financial institutions have experienced multiple breaches and risks. To proactively identify and address these challenges, it is essential for such institutions to establish a framework of regular or periodic Data Protection Impact Assessments (DPIAs), Access Review and other IT Security Audits on the data privacy practices assessing and mitigating the privacy risks associated with data processing as defined by the DPDPA. Implementation of Independent audits around data privacy of the financial institutions are one of the key controls that directly increase the trust of the data principal.

The convergence of IT security and personal data protection under the DPDPA 2023 underscores the inseparable nature of these disciplines. Organisations that recognise this synergy and invest in a harmonised approach will not only ensure compliance but also fortify their reputation as custodians of data integrity and privacy in an increasingly digital world. Through this strategic alignment, the safeguards designed to protect data will simultaneously protect the trust of individuals and stakeholders.



Product management

Product management must infuse designs with data protection, transparency and user rights. Priorities include integrating "privacy by design", strong consent mechanisms, clear user control, transparent communication, well-defined data usage policies, and data protection and retention strategies. These adaptations ensure products align with DPDPA principles.

Outlined below are several critical considerations that are devised to ensure the safety of users' personal data. These factors should be meticulously considered during the design and oversight of products, including those catering to or collecting data from minors, in alignment with the protocols stipulated by the DPDPA. This alignment aims to foster trust among stakeholders, encouraging their active involvement in advancing the Digital India Initiative.

- **Data rationalisation:** Organisations should limit their data collection and storage endeavours to only the essential information required for the optimal functionality of their products. The accumulation of surplus or unrelated data must be actively discouraged by the data fiduciary at a policy level within each company. This practice not only fosters customer confidence in data sharing, it will also reduce the data privacy risk management resulting in reduction in efforts and other resources.
- **Explicit consent and transparency:** Obtain clear and informed consent from users before collecting their data and only for business requirements. Users should know why their data is being collected and how it will be used. Provide clear and easily accessible privacy policies and terms of use that outline how the data is collected, processed, and shared. It is critical for users to further understand the implications of data sharing so that they can take an informed decision. Age is a factor for required consents. DPDPA allows digital personal data to be transmitted and stored abroad, given its connection to providing services to data principals. As a result, data fiduciaries must specify the nature of data, relevance, and processing purpose. While the Act allows cross border data transfers to certain jurisdictions (to be notified later) with explicit consent from the data principal, there are extant sectoral regulatory instructions on such cross border data flows that the financial institutions need to consider to ensure compliance with regulatory instructions and the Act. Strict requirements around consent and transparency is likely to impact the new customer acquisition process, since products need to be modified to comply with the Act. It is also likely to impact business growth as some of the customers may not want to go ahead with the product if they are not comfortable in accepting the policy requirements. Financial institutions may be further required to take revised consents with the required transparency from existing customers. This can result in certain customers declining consent basis the clarity on how the personal data will be used by these financial institutions and customers may do their own risk benefit analysis whether to use the product or not.
- **Pseudonymisation:** Going forward, a process similar to the tokenisation implemented by financial institutions for credit card and other financial data may be required to be implemented. This will be necessary for personally identifiable information (PII) collected as part of product creation and monitoring to reduce the risk of identifying individuals while maintaining their personal data utility and even in the unforeseen scenarios of cyber-attacks. This is expected to increase the cost of doing business for financial institutions.
- **Users control on the data shared:** Providing user the ability to control their data shared with the data fiduciary showcases the importance of rights of data principal on their personal data. This may include options to edit or delete their data, manage their preferences, and opt-out of certain data collection activities. This again requires financial institutions to modify existing product configurations to manage these new requirements and may also need to identify ways to be built for the products which are currently under development.
- **User data security:** The requirements around implementation of robust security protocols to safeguard user's personal data from breaches has been the forefront. This involves encryption, access controls, regular security audits, and patches for vulnerabilities. The policies of the data fiduciary may include synopsis on the controls of the organisation specifying the access to user data to only those who need it for legitimate purposes and implement role-based access controls to prevent unauthorised access. These specific requirements will have an impact on the current policies, systems, procedures, customer contracts, learning & development, audit/control monitoring and the existing IT security framework. A current state assessment needs to be done to address the above by setting up defined timelines for the implementation.
- **Data management:** The products should clearly define data collection processes — how long data will be retained by the data fiduciary and when the same will or should be deleted. The companies must erase personal data as soon as the purpose has been met and retention is not necessary for legal purposes (storage limitation). This once defined should be adequately adhered to on a continuous basis. All the data that have met their purpose should be deleted to minimise the risk of data breaches.

- **Third-party management:** In instances where the product architecture incorporates third-party services to retrieve data from data principals, it is imperative to ascertain that these service providers also maintain rigorous data privacy protocols. The service provider agreements should document procedures to be followed and outline their responsibilities regarding personal data protection. The data fiduciaries will accordingly be required to review their existing third-party agreements to incorporate new requirements such as data collection and processing. The data fiduciaries will have to include clauses with negative incentives in the form of penalties against each of those requirements of the DPDPA framework. Any breach on the personal data will impact data fiduciaries in terms of penalties and loss of reputation, among others.

The change in perspective from collecting all possible user touchpoints to collecting the relevant data will change product development and management cycle. It will affect the information the user must provide during customer onboarding, customer lifecycle management, cross selling activities to name a few. In times to come, we shall see the product teams to incorporate these changes and evolve a suitable approach to manage compliances with DPDPA while ensuring product innovation continues as is.

Customer lifecycle management

- DPDPA introduces fresh mandates, rights, and duties for firms managing customer data across their journey. This spans customer onboarding, risk evaluation, profiling, marketing, engagement, service, data rights management, and cessation of customer relationships. This requires substantial transformation in the approach to customer lifecycle management. The DPDPA has introduced stringent guidelines and obligations to ensure the protection of individuals' personal data. This legal framework has far-reaching implications for various sectors, including how organisations manage the lifecycle of their customers.
- Customer lifecycle stages
  - **Customer acquisition:** The DPDPA emphasises on the importance of obtaining explicit and informed consent from individuals before collecting their personal data. This directly impacts customer acquisition strategies, as organisations must now ensure that their data collection practices align with the Act's regulations. Since financial institutions significantly outsource customer acquisition processes, the acquisition journey becomes sensitive and important since data must be shared and captured carefully most likely in a masked manner.
  - **Customer onboarding:** During the onboarding process, organisations must communicate their data usage policies clearly and provide individuals with the option to grant or deny consent. The consent must be provided in multiple languages, to ensure the customer understands what he/she is agreeing to. This stage becomes a crucial point for organisations to showcase their commitment to data protection, as individuals need to be well-informed about how their data will be utilised. The companies must capture and store only relevant data and build reasonable security safeguards to prevent a data breach.
  - **Customer service:** When businesses help their customers with any issues or questions, they now have a bigger responsibility to keep the information accurate and secure. The way financial institutions handle customer inquiries and address problems will require a significant change. The financial institutions need to ensure that the data they capture is accurate, up to date and well-protected. Organisations often outsource customer support functions and, in such cases, sharing of customer data, processing and storage by the third-party must be in accordance with the provisions of the Act and should be monitored regularly.
  - **Customer retention:** Organisations must adhere to the principle of data minimisation, collecting only the data necessary for providing their services. This impacts customer retention strategies by fostering an environment where individuals feel confident that their data is handled responsibly and is not retained unnecessarily. It is an opportunity for businesses to differentiate themselves by demonstrating commitment to customer privacy.
  - **Customer loyalty:** As businesses navigate the landscape shaped by the DPDP Act 2023, those who can prioritise data protection can foster stronger customer loyalty. When individuals witness that their personal data is treated with respect and care, they are more likely to remain loyal to institutions that prioritise their privacy.

The DPDPA will significantly alter the way organisations approach customer lifecycle management. By placing data protection and privacy at the forefront, the Act shall prompt businesses to revaluate their data collection, usage, and retention practices. This has far-reaching implications on customer acquisition, onboarding, servicing, retention and loyalty strategies. The Act necessitates transparency, informed consent, and data accuracy throughout the customer journey. For businesses that embrace these principles, the Act becomes an opportunity to build trust, differentiate themselves and foster lasting customer relationships.

Outsourcing

- **Roles and responsibilities:** Financial services firms frequently outsource tasks and engage with Fintechs. Current regulator-issued guidelines address outsourcing risks, emphasising customer data governance. However, DPDPA enforces data fiduciaries' substantial compliance duties surpassing present regulatory requirements. Consequently, firms will likely need to reassess outsourcing, scrutinise outsourced customer data processes, and realign governance structures for compliance management. Existing agreements will need to be scrutinised to identify any loopholes and contracting would need to consequently be re-visited. Roles and responsibilities of both the data fiduciaries (DFs) and the data processors (DPs) would need to be distinctly defined.
- **Enhanced control and oversight:** Data fiduciaries (DFs) will be ultimately responsible for maintenance of complete, accurate and consistent data. While they may appoint a data processor for processing of data, the ownership of compliance stays with the DF. This will necessitate the DF to ensure that a valid contract with adequate clauses from a compliance and regulatory adherence standpoint are built in into the agreement with the data processor. The DFs will need to put controls in place to ensure that periodic reviews are conducted by the data processors and sufficient assurance is provided to the DF. While the RBI outsourcing norms do mandate several robust controls, the DPDPA penalties would further act as disincentive and nudge DFs to ensure outsourcing risks are managed more effectively.
- **Vendor risk management:** Risk management practice with respect to outsourcing now becomes pivotal as associated regulatory and reputational risks are expected to increase for the DFs. DFs will not only need to conduct periodic review, data audits/impact assessments themselves but also mandate their data processors to provide periodic compliance certificates, evidence of controls established and reports of independent audits conducted. Process and controls around consent management, issuance of notice, erasure of data post revocation of consent (subject to the PMLA provisions on data storage) will need to be robust and monitored regularly to ensure overall compliance. The cost of compliance will certainly increase for the DPs and hence, they may further re-look at the financial viability and consequently the agreements entered with DFs.

The Act states that the Central government may notify any data fiduciary or a class of data fiduciaries as significant. This shall primarily be based on the volume and sensitivity of personal data processed, and potential risk and impact associated. We foresee that given the volume and nature of data processed, several key players within the financial services domain will be identified as significant data fiduciaries (SDF). While SDFs will also need to appoint a data protection officer and set up a grievance redressal mechanism, the act mandates them to appoint an independent data auditor and conduct periodic data protection impact assessments. SDFs will not only need to conduct sufficient due diligence to outsource or appoint an independent auditor but will also need to re-look at existing audits from a scoping and coverage standpoint.

Increased compliance for Fintechs

Indian Fintechs have been rapidly transforming the financial services landscape by partnering with incumbent regulated entities (RE) and leveraging customer data to deliver hyper-customised products to them at affordable prices, digitally. Under DPDPA 2023, Fintechs will be classified as 'data processors' and will have to comply with requirements that apply to data fiduciaries. In future, the RE-Fintech partnership model will be reset, where REs will now exercise increased oversight on data governance practices of Fintechs. Those Fintechs with superior data governance processes will be sought-after partners for the REs and will thrive under the new data regime. Key areas where Fintechs will require to assess impact of DPDPA are:

- **Data inventory and mapping:** Fintechs, during their interaction with the customer, collect information about the customer, especially through their mobile applications. Fintechs will have to undertake a comprehensive assessment of their processes to understand the personal data being collected, processed, and stored by them. This assessment will help fintechs identify the types of data they are handling, where the data is located, how it is used, and with whom it is shared. To do so, they will have to identify data sources, categorise data into personal identifiable information (PII), behavioural, financial, etc., identify data sharing instances and determine and align data retention periods with DPDPA 2023.
- **Data minimisation and purpose limitation:** With the DPDPA 2023 coming into force, Fintechs will be required to follow the principle of data minimisation and purpose limitation. Once data inventory and mapping has been carried out, Fintechs will have to further identify data that is essential for specific, well-defined purposes which have sound legal basis for collection. This assessment will help Fintechs streamline data collection and reduce the risk of unauthorised access or misuse of sensitive information.
- **Enhanced transparency and consent mechanisms:** Fintechs, as partners of incumbent REs who are the ultimate data fiduciary under the DPDPA 2023, will be required to make significant changes to their design of customer lifecycle journey. One fundamental shift lies in the realm of purpose, notice, and consent. Fintech entities will be required to secure explicit, clear, and unambiguous consent from individuals whose data they handle. This emphasises transparency, enabling individuals to make informed choices about the use of their personal information. Additionally, fintech companies will be required to provide easily understandable notices and consent requests in multiple languages, ensuring accessibility to a diverse user base. This new level of transparency will not only build trust between users and fintech platforms but shall also significantly reduce instances of data misuse. In the unfortunate event of a breach occurring, the DPDP Act 2023 mandates timely reporting to both the Data Protection Board and the affected individuals ensuring accountability and transparency within Fintech companies.
- **Cross-border data transfers and security measures:** Fintech operations often involve cross-border data transfers. The DPDPA 2023 has laid down specific requirements for such transfers, ensuring that data moving across international boundaries is adequately protected. Fintech companies will be required to implement appropriate security measures to prevent data breaches and unauthorised access. This is likely to hasten the adoption of robust cybersecurity protocols within the Fintech sector. The policy of cross-border data transfers strikes a balance between promoting international data flows essential for Fintech innovation and ensuring that data remains protected even beyond national borders. This is a pivotal step toward fortifying data protection practices, fostering user trust, and driving responsible innovation within the dynamic landscape of financial technology.
- **Accountability through data protection officers:** The DPDPA 2023 recognises the different scales of data processing carried out by fintech companies. Those dealing with substantial volumes of personal data may be designated as significant data fiduciaries. This classification entails increased responsibilities, including the appointment of data protection officers (DPOs) as second line of defence within Fintech companies. These experts will be tasked with overseeing data protection strategies, conducting audits, and acting as a bridge between the company, its users, and regulatory authorities. These DPOs will not only ensure adherence to the DPDP Act 2023 but also foster a proactive approach to data protection.


Retention
81%
69%
85%
Profit and Loss summary
Last 24 Hours

Implications on global capability centres (GCCs)

Several banks that operate across the globe have offshore units or GCCs based in India. While initially they may have been set up as a cost optimisation measure, gradually they have become centers that provide valued services from both a skillset as well as technology standpoint. According to research, there are close to 1600 GCCs in India across various locations, which have been increasing exponentially. The BFSI industry has also evolved and transformed its global service delivery model by establishing these Global Capability Centers. Given that the DPDPA is applicable to both data processed in India and abroad in connection to activities based in India, two key areas or consideration points for GCCs in the financial services domain are discussed here.

- **Identification of cross border data that falls under the gamut of the Act:** Each GCC works on a slightly unique business model especially when it pertains to processing or utilising data. There is a considerable number of cross border data that GCCs in India will have to scrutinise and review to identify data sets that fall under the gamut of this Act. For personal data that pertain to individuals, products, processes or regulators based outside India, but which is processed (as per DPDPA 2023) in India, the GCCs will need to set up a robust control framework to ensure compliance with the said provisions. Furthermore, there will be redundancies and overlaps especially for those GCCs where data sources are both from within and outside India. While the Central Government should shortly issue FAQs addressing the cross-border transfer of data, GCCs will need to initiate their analysis in primarily segregating data sets into those for which compliance is to be ensured and the rest, if any, which fall outside the scope of this Act.
- **User access management of personal data of employees onboarded by GCCs in India:** The second key aspect will be around obtaining, managing, and storing of the personal data of personnel employed by GCCs in India. According to a report by NASSCOM, nearly 21% of all GCC employees in India work in the BFSI sector. Given the significant number of people employed by GCCs in India, there is expected to be a significant amount of personal data, which will be made available to entities. While it will be relatively simple to get consent, for management of the personal data for such a large repository of employees with ongoing attrition, constant modifications will be a key area of focus. Critical employee data necessary for onboarding will need to be identified to reduce the amount of personal data obtained and stored. While data localisation norms are prevalent, GCCs will further need to evaluate the level of access granted to a data processor who is likely to be appointed and extent of personal data shared outside India. User access management for personal data of personnel working for GCCs will need to be periodically reviewed to ensure there is no misuse/unauthorised access or potential non-compliances and consequent penalties.

Conclusion

The DPDPA 2023 emerges as a watershed moment for the country and provides individuals the opportunity to exercise control over their data. This legislation redefines the relationship between consumers and businesses, emphasising transparency. Beyond compliance, the DPDPA underscores the need for a cultural shift towards valuing data privacy. Society must recognise the worth of data and advocate for responsible data practices as a collective value. With the passing of the legislation, financial institutions have now emerged as custodians of customer data. By adhering to DPDPA's principles, these institutions become trusted data stewards, fostering innovation and ethical data management. The DPDP Act of 2023 stands as a testament to the evolving regulatory guidelines in the Fintech sector. By mandating transparency, consent, and robust security measures, it has elevated compliance standards for Fintech companies. Through data minimisation, purpose limitation, and cross-border data transfer regulations, the Act has struck a balance between innovation and user protection.

The DPDP Act 2023 has significant impact. It compels organisations to elevate their data protection practices, which in turn enhances customer trust, satisfaction and loyalty. As businesses adapt to the Act's requirements, they simultaneously strengthen their relationships with customers by prioritising their privacy and data security. This synergy between data protection and lifecycle management exemplifies the Act's expanded goal of establishing a privacy-centric digital ecosystem.

The DPDPA 2023 is more than a regulation. It offers a unique opportunity for financial institutions to enhance data security, build customer trust, and lead the way for responsible data management practices. By embracing the Act's provisions, financial services companies can not only navigate the evolving regulatory landscape but also position themselves as guardians of customer data in an increasingly interconnected and data-driven world.

Key definitions

I	Data Fiduciary	Any person who alone or in conjunction with other person determines the purpose and means of processing of personal data;
II	Data Principal	The individual to whom the personal data relates and where such individual is - **(i) a child, includes the parents or lawful guardian of such a child.** (ii) a person with disability, includes her lawful guardian, acting on her behalf
III	Data Processor	Any person who processes personal data on behalf of a Data Fiduciary

Glossary

DPDPA	Digital Personal Data Protection Act
FS	Financial Services
PMLA	Prevention of Money Laundering Act
IT Act	Information Technology Act, 2000
RBI	Reserve Bank of India
SEBI	Securities and Exchange Board of India
IRDAI	Insurance Regulatory and Development Authority of India
BCSBI	Banking Codes and Standards Board of India
DLA	Digital Lending Applications
DPB	Data Protection Board
KYC	Know Your Customer
RE	Regulated Entities
DPIAs	Data Protection Impact Assessments
CCM	Continuous Control Monitoring
DFs	Data Fiduciaries
DPs	Data Processors
SDF	Significant Data Fiduciaries
DPO	Data Protection Officer

Acknowledgements

Authors

Deepankar Sanwalka
Senior Partner – National Management

Vivek Iyer
Partner – Fintech Industry leader

Rohan Lakhaiyar
Partner – Financial Services Risk

Akshay Garkel
Partner – Cyber leader

Dharmendra Jhamb
Partner – Digital Natives

Research & analysis

Yogesh Purohit
Associate Director – Financial Services Risk

Viraj Parikh
Manager – Financial Services Risk

Ramanujam Krishnan
Manager – Markets Ecosystems

Aakriti Malik
Assistant Manager – Markets Ecosystems

For queries, please contact

Vivek Iyer
Partner – Fintech Industry leader
Vivek.iyer@in.gt.com

Rohan Lakhaiyar
Partner – Financial Services Risk
rohan.lakhaiyar@in.gt.com

Editorial review	Design
Runa Dasgupta	Vaibhav Bhargava

Great Place To Work. Certified NOV 2022 - NOV 2023 INDIA

Best Workplaces™ in Professional Services

Great Place To Work. INDIA 2023

We are
Shaping Vibrant Bharat

A member of Grant Thornton International Ltd., Grant Thornton Bharat is at the forefront of helping reshape the values in the profession. We are helping shape various industry ecosystems through our work across Assurance, Tax, Risk, Transactions, Technology and Consulting, and are going beyond to shape a more **#VibrantBharat.**

Our offices in India

Ahmedabad • Bengaluru • Chandigarh • Chennai • Dehradun • Delhi • Gurgaon • Hyderabad • Kochi • Kolkata • Mumbai • Noida • Pune

Scan QR code to see our office addresses

www.grantthornton.in

Connect with us on

@Grant-Thornton-Bharat-LLP

@GrantThorntonBharat

@GrantThornton_Bharat

@GrantThorntonIN

@GrantThorntonBharatLLP

GTBharat@in.gt.com

© 2023 Grant Thornton Bharat LLP. All rights reserved.

"Grant Thornton Bharat" means Grant Thornton Advisory Private Limited, the sole member firm of Grant Thornton International Limited (UK) in India, and those legal entities which are its related parties as defined by the Companies Act, 2013, including Grant Thornton Bharat LLP.

Grant Thornton Bharat LLP, formerly Grant Thornton India LLP, is registered with limited liability with identity number AAA-7677 and has its registered office at L-41 Connaught Circus, New Delhi, 110001.

References to Grant Thornton are to Grant Thornton International Ltd. (Grant Thornton International) or its member firms. Grant Thornton International and the member firms are not a worldwide partnership. Services are delivered independently by the member firms.