



Digital Personal Data Protection Act

Edition XI

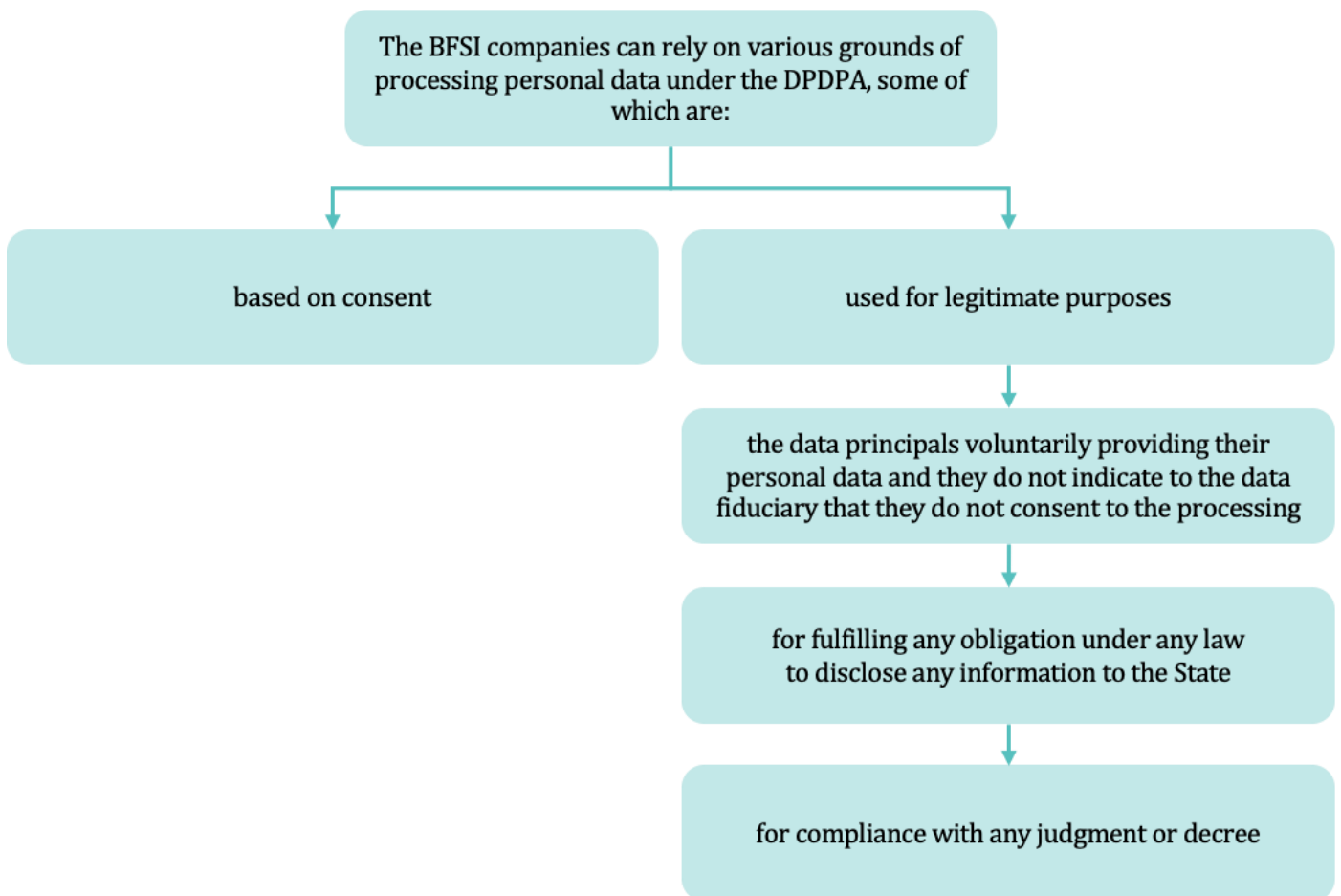
December 2024

Impact of data protection laws on the Banking, Financial Services and Insurance sector

In this Prism, we analyse the impact of the Digital Personal Data Protection Act, 2023 (“**DPDPA**”) on the Banking, Financial Services, and Insurance (“**BFSI**”) sectors. The application of DPDPA to the BFSI sector poses unique challenges and opportunities to the existing, well-defined regulatory landscape. With robust frameworks already prescribed by the Reserve Bank of India (“**RBI**”), the Insurance Regulatory and Development Authority of India (“**IRDAI**”), and the Securities and Exchange Board of India (“**SEBI**”), the BFSI sector already adheres to stringent data protection norms. However, the DPDPA introduces broader principles that address gaps, particularly in areas such as individual rights and consent specificity. Below, we analyse key areas of overlap, divergence and harmonisation.

Grounds for processing personal data

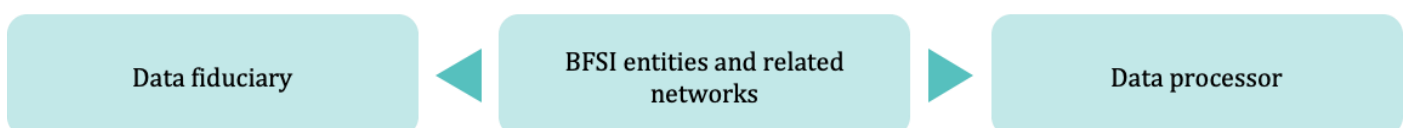
Under the DPDPA there are 2 (two) valid grounds for processing: (a) consent; and (b) for legitimate purposes. The BFSI sector has long operated on the principle of informed consent, as emphasised by RBI, SEBI, and IRDAI guidelines. For example, the RBI’s KYC Directions ensure that individuals provide explicit consent for data collection during onboarding processes. However, these consent mechanisms often encompass broad purposes, such as transaction facilitation or compliance, without specification. The DPDPA refines the concept of consent, emphasising explicit, specific, and purpose-bound agreements. This adds a layer of granularity that BFSI entities must integrate into their consent frameworks. This requires operational shifts, such as updating consent forms and refining digital interfaces to ensure clarity and compliance.



The concept of a consent manager under the DPDPA could be similar to the RBI's Account Aggregator ("AA") framework, introduced under the Master Directions - Non-Banking Financial Company - Account Aggregators (Reserve Bank) Directions, 2016. This framework envisioned intermediaries facilitating secure, user-controlled sharing of financial data. These AAs act as consent managers, ensuring that individuals retain control over their data while enabling seamless data sharing between financial institutions. Under the DPDPA, the consent manager concept is expanded to apply across sectors, providing tools for users to manage and revoke consent efficiently.

The existing BFSI regulations allow data processing under legal mandates, such as anti-money laundering requirements or fraud detection. This is broadly in line with processing personal data, without consent, for legitimate uses such as compliance with laws of India or to comply with a judgement, decree or order issued under Indian laws, as given under the DPDPA. Entities operating in the BFSI sector may sometimes need to disclose or share data for compliance with foreign regulations or orders or to work with other companies that are required to meet their foreign obligations. In such cases the entities would need to carefully consider the grounds for such data processing.

Role in processing personal data



Under the DPDPA, the BFSI entities and other entities in the financial ecosystem cannot operate under a fixed assumption that they will always fall under a single role, be it data fiduciary or processor. Their role under the DPDPA would depend on the specific context of data processing in each use case. This fluidity of roles necessitates a case-by-

case evaluation, considering factors such as the origin of data, contractual obligations and the control exercised over the data's use. Therefore, all organisations in the financial ecosystem must meticulously analyse their data flows and processing arrangements to correctly identify their role which would in turn influence the kind of obligations they would have under the DPDPA.

Enhanced obligations for BFSI entities

Under the DPDPA, it is highly likely that BFSI entities could be classified as Significant Data Fiduciaries ("SDFs") given that their core operations involve processing sensitive data and the potential risks to individual's privacy in the event of a breach. These entities may collect and process data like financial details, aadhaar, permanent account number and biometric information for purposes such as 'know your customer' compliance, credit approvals and fraud prevention. If designated as SDFs, BFSI entities will be required to comply with enhanced obligations, including conducting Data Protection Impact Assessments (DPIAs), appointing a Data Protection Officer (DPO) and undergoing independent data audits.

Existing regulations, such as RBI's guidelines on cybersecurity, SEBI's data handling norms for intermediaries and IRDAI's privacy-related directives, further reinforce the specific responsibilities of BFSI organisations. The sector's reliance on digital platforms, artificial intelligence tools and data-driven decision-making makes compliance with the fiduciary obligations under the DPDPA a natural extension of their regulatory obligations. These entities are well-positioned to meet the core requirements for lawful, fair and transparent data processing mandated by the DPDPA.

For entities in the BFSI sector, this would mean aligning their compliance efforts under the DPDPA with existing regulatory frameworks while investing in robust data governance mechanisms. Proactively preparing for this designation will not only ensure compliance but also build greater trust with customers and stakeholders in an increasingly data-driven financial environment.

Cross-border transactions and DPDPA

The Central Government, by notification may restrict transfer of personal data outside India to certain countries or territories. The DPDPA mentions that sectoral legislations will supersede the provisions of the DPDPA where there is transfer of personal data outside India. In the BFSI sector there are various sectoral laws that mandate data localisation and regulate the transfer of personal data outside India. These sectoral requirements add layers of complexity to cross-border data processing and necessitate BFSI entities to implement robust data governance frameworks.

For instance, the RBI mandates that payment system data be stored in India, impacting payment intermediaries and financial institutions handling transaction data. Similarly, insurance companies must adhere to the regulations of the IRDAI, which imposes specific restrictions on cross-border data flows.

To comply with both the DPDPA and sectoral mandates, the BFSI institutions must assess their data processing activities, ensure localisation requirements are met and establish agreements with service providers detailing compliance with cross-border data transfer rules. Furthermore, leveraging privacy-enhancing technologies such as encryption and anonymisation can mitigate risks associated with permitted international data transfers while adhering to regulatory expectations.

Consistency between DPDPA and sectoral regulations

While RBI, IRDAI and SEBI frameworks emphasise data security and governance, they lack comprehensive mechanisms for addressing individual rights. The DPDPA introduces rights for individuals, including the right to access, correction and erasure, which BFSI entities must now accommodate. Requests for data erasure may specifically pose challenges due to retention obligations mandated under different applicable laws.

While sectoral regulations mandate privacy disclosures, the DPDPA requires detailed privacy notices that explicitly outline data processing purposes, storage durations and cross-border transfer mechanisms. This demands a review of privacy policies, ensuring they are comprehensive yet easily comprehensible.

The DPDPA complements the BFSI sector's existing frameworks, addressing gaps in individual-centric rights and introducing a harmonised approach to global data governance. However, it also presents challenges in reconciling the variance in the sectoral guidelines and DPDPA.

Infotech Practice (Privacy and Data Protection)

Our team understands the importance of data privacy in today's digitally interconnected world. We have dedicated our practice to ensuring that your and your customers' personal and business data remains secure, compliant, and respects the sovereignty of individuals and jurisdictions globally.

We prioritise creating bespoke solutions tailored to your business needs. We recognise that every business has unique data privacy challenges, and we use our deep understanding of international and domestic regulations to provide you with the most effective and robust legal strategies. JSA provides advice on highly sophisticated data management, data security and privacy issues. Our depth of experience gives our clients the crucial advantage of consistent and comprehensive, yet practical advice. Our Technology Law Practice group has successfully worked with several multinational organisations for the structuring and roll-out of privacy and information-security programs. We have carried out audit and risk assessments, customised global privacy and information management policies, helped create international data transfer strategies, structure and negotiate complex international data transfer agreements.

This Prism has been prepared by:



Akshaya Suresh
Partner



Drishya A. Kamath
Associate

		
18 Practices and 41 Ranked Lawyers	7 Ranked Practices, 16 Ranked Lawyers ----- Elite – Band 1 - Corporate/ M&A Practice ----- 3 Band 1 Practices ----- 4 Band 1 Lawyers, 1 Eminent Practitioner	12 Practices and 50 Ranked Lawyers
		
14 Practices and 38 Ranked Lawyers		
		
20 Practices and 22 Ranked Lawyers	Ranked Among Top 5 Law Firms in India for ESG Practice	Recognised in World's 100 best competition practices of 2025
		
Among Top 7 Best Overall Law Firms in India and 11 Ranked Practices ----- 11 winning Deals in IBLJ Deals of the Year ----- 11 A List Lawyers in IBLJ A-List - 2024	Asia M&A Ranking 2024 – Tier 1 ----- Employer of Choice 2024 ----- Energy and Resources Law Firm of the Year 2024 ----- Litigation Law Firm of the Year 2024 ----- Innovative Technologies Law Firm of the Year 2023 ----- Banking & Financial Services Law Firm of the Year 2022	Ranked #1 The Vahura Best Law Firms to Work Report, 2022 ----- Top 10 Best Law Firms for Women in 2022
		
		7 Practices and 3 Ranked Lawyers

For more details, please contact km@jsalaw.com

www.jsalaw.com



Ahmedabad | Bengaluru | Chennai | Gurugram | Hyderabad | Mumbai | New Delhi



This prism is not an advertisement or any form of solicitation and should not be construed as such. This prism has been prepared for general information purposes only. Nothing in this prism constitutes professional advice or a legal opinion. You should obtain appropriate professional advice before making any business, legal or other decisions. JSA and the authors of this prism disclaim all and any liability to any person who takes any decision based on this publication.