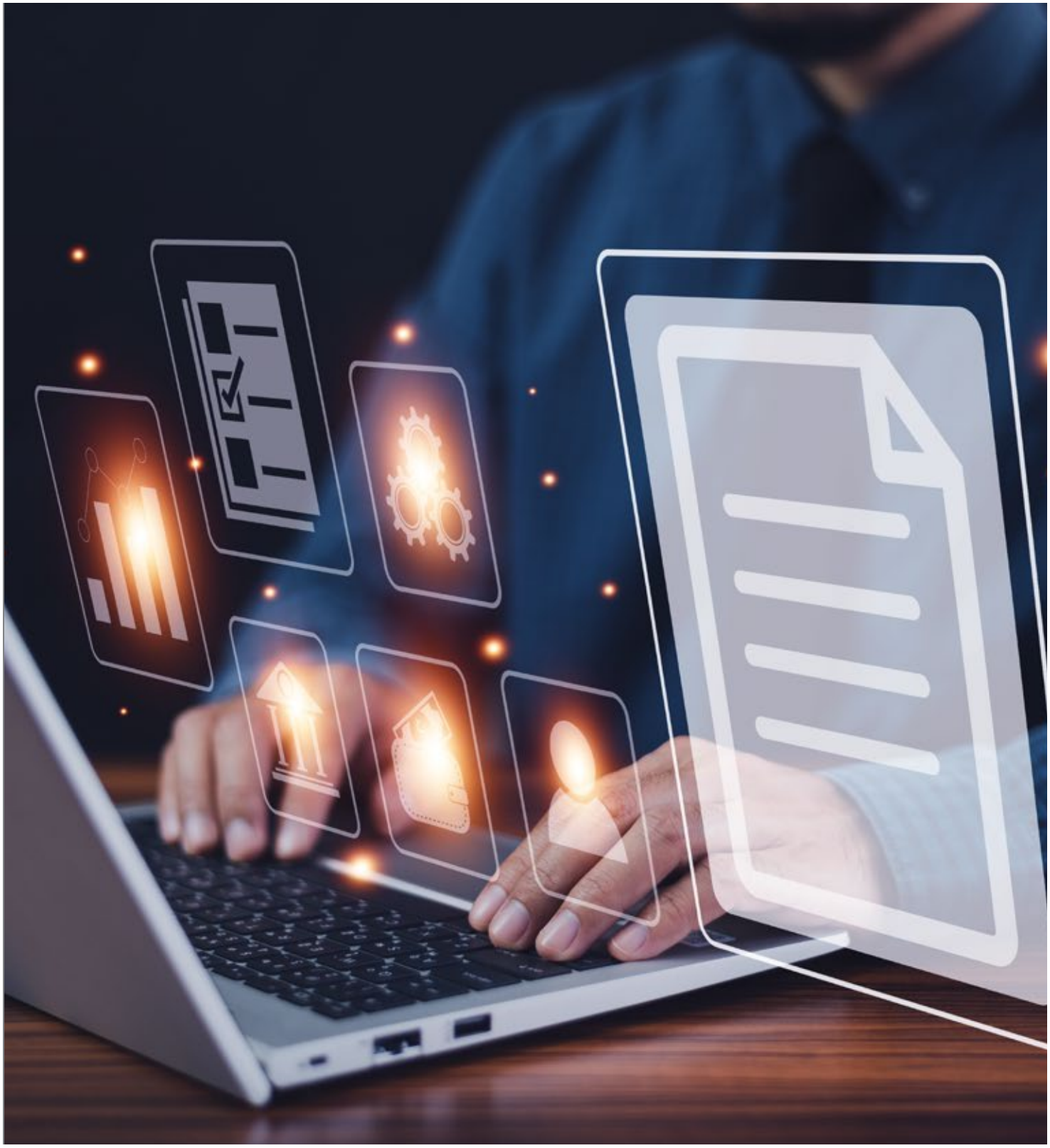
UJA
Audit • Tax • Legal • Advisory

Legal Chronicle

OCTOBER 2025



India | Japan | Italy | Spain | France | Germany | UAE

Dear Reader,

The Legal Department at UJA is delighted to impart certain legal knowledge as construed under the Legal Chronicle to keep the readers aware of the recent updates and developments that revolve around various aspects of the law. Our goal is to enable our readers to develop a sense of familiarity with the complexities of Indian as well as international law.

In this edition of Legal Chronicle, we present an insightful overview of the evolving compliance framework under the Digital Personal Data Protection Act, 2023 (DPDP Act), a legislation of critical importance for organizations processing personal data in India. With the growing reliance on data-driven operations, it has become essential for businesses to embed privacy safeguards into their processes and systems. This article thus examines the role of the Business Requirement Document (BRD) and the Consent Management System (CMS) as practical tools for implementing compliance with the DPDP Act. It further explores the importance of aligning business processes with legal obligations, the integration of BRD and CMS and the challenges and solutions in operationalizing data protection by design.

We hope that this edition creates a sense of enthusiasm for our readers and successfully delivers the plethora of legal knowledge as intended. In case you have any feedback or need us to include any information to make this issue more informative, please feel free to write to us at legal@uja.in.

Contents

Business Requirement Document (BRD) and the Consent Management System (CMS) under the DPDP Act, 2023

1. Introduction

The advent of the Digital Personal Data Protection Act, 2023 (DPDP Act) marks a significant step in India's data protection regime, laying down comprehensive obligations for organizations that process personal data. With consent and accountability at its core, the Act requires businesses to embed privacy safeguards into their operational and technological frameworks. In this context, compliance is not merely a legal formality but a strategic necessity for fostering trust, ensuring data security and aligning with global standards of privacy governance. Two critical tools that enable organizations to operationalize compliance are the Business Requirement Document (BRD) and the Consent Management System (CMS). While the BRD provides a structured framework for capturing business and legal requirements relating to data processing, the CMS offers mechanisms to obtain, record and manage consent effectively. Together, they provide a holistic compliance framework that integrates business needs with legal mandates.

2. Overview of the DPDP Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act), is India's first comprehensive legislation regulating the processing of digital personal data. It places obligations on Data Fiduciaries and Data Processors to ensure that personal data is collected, stored and processed lawfully, with due respect to the rights of individuals. In practice, the DPDP Act emphasizes principles such as lawful processing, obtaining valid consent, limiting the use of data to specific purposes and ensuring adequate security safeguards. It also provides individuals with greater control over their personal information by granting rights to access, correct or erase their data. To oversee implementation, the Act establishes a regulatory authority that can monitor compliance, address grievances and impose penalties for non-compliance.

a) Importance of compliance for organizations processing personal data

The Digital Personal Data Protection Act, 2023 (DPDP Act) establishes a comprehensive framework for safeguarding personal data and imposes obligations on organizations, known as Data Fiduciaries, that process such data. Compliance is crucial not only to avoid statutory penalties but also to build trust and transparency with data principles whose information is being collected and processed. Non-compliance may lead to significant financial liability, reputational harm and even business disruption. By ensuring adherence to the DPDP Act, organizations demonstrate accountability, maintain the confidentiality and integrity of personal data and align themselves with global standards of privacy protection.

b) Objective of linking BRD and CMS to DPDP compliance

To effectively operationalize compliance, organizations must integrate the Business Requirement Document (BRD) and the Compliance Management System (CMS) with the obligations under the DPDP Act. The BRD sets out the functional and technical requirements of data collection, storage, transfer and usage processes, ensuring that privacy considerations are embedded at the design stage itself. On the other hand, CMS helps to monitor, evaluate and report compliance with legal and organizational policies. Linking the BRD with the CMS ensures that compliance is not a one-time exercise but an ongoing, auditable process, allowing organizations to demonstrate accountability, quickly respond to data breaches and maintain robust documentation in case of regulatory scrutiny.

3. Business Requirement Document (BRD) under DPDP Act, 2023

a) Definition of BRD in the compliance context

Business Requirement Document (BRD) serves as a foundational document that outlines how an organization intends to collect, store, process and manage personal data in alignment with statutory requirements. It acts as a bridge between legal obligations and business operations, ensuring that data protection principles such as consent, purpose limitation, data minimization and lawful processing are embedded into the organization's processes and systems from the outset. The BRD thus becomes an essential compliance tool, guiding business teams, IT departments and legal/compliance units in implementing data protection by design and by default.

b) Key Elements of BRD

- The BRD under the DPDP Act should comprehensively outline the key compliance elements necessary for lawful processing of personal data. It should begin by identifying the categories of personal data to be collected, such as name, contact details, financial information or sensitive personal data.
- The BRD must clearly specify the purpose of collection to ensure adherence to the principle of purpose limitation and avoid unauthorized use. It should also detail the consent mechanism, including how valid and informed consent from data principles will be obtained, recorded and managed.
- Further, the document must describe the data processing activities, covering storage, transfer, sharing with third parties and the eventual deletion of data.

- To safeguard confidentiality and integrity, the BRD should set out appropriate technical and organizational security measures such as encryption, access controls and audit trails. Additionally, it must define policies on data retention and deletion, ensuring that personal data is retained only for as long as necessary and securely disposed of thereafter.

- Finally, the BRD should clearly allocate roles and responsibilities among the data fiduciary, data processors and compliance officers, thereby establishing accountability and enabling effective implementation of the DPDP Act.

c) Scope of Data Processing

The categories of personal data collected typically include basic identifiers such as name and email address, along with sensitive data such as financial details, biometric information and other relevant records, depending on the nature of the business. Such data is collected for specific purposes, including customer service, marketing initiatives, human resources management and regulatory compliance. Once collected, the data may be subject to various processing activities, such as secure storage, transfer to third parties or affiliates for legitimate business needs and profiling for service enhancement, provided that these activities remain within the scope of consent and the lawful purposes disclosed to the Data Principal.

d) Stakeholders

Within the framework of the DPDP Act, the primary responsibility lies with the Data Fiduciary, which is the entity that determines the purpose and means of processing personal data. Supporting this role are Data Processors, who are third-party entities engaged to process data on behalf of the Data Fiduciary, subject to contractual and legal safeguards. In cases where an organization qualifies as a Significant Data Fiduciary, the appointment of a Data Protection Officer (DPO) becomes mandatory to oversee compliance and act as a point of contact for grievance redressal. Alongside these roles, internal stakeholders such as business teams, IT departments and legal or compliance units play a crucial part in implementing data protection measures, ensuring that the organization's processing activities remain aligned with statutory obligations.

4. Consent Management System (CMS) under DPDP Act,2023

a. Definition of CMS

A Consent Management System (CMS) under the Digital Personal Data Protection Act, 2023, is a structured framework that enables organizations to obtain, record, manage and track the consent of data principals in a transparent and auditable manner. Since the DPDP Act makes consent the primary ground for processing personal data, the CMS ensures that consent is free, informed, specific, unconditional and capable of being withdrawn at any time. It provides businesses with the technological and procedural tools to demonstrate compliance, while also empowering individuals with greater control over their personal data.

5. Integration of BRD and CMS

The Business Requirement Document (BRD) and the Consent Management System (CMS) work best when integrated into a unified compliance strategy. While the BRD defines what personal data is collected, why it is collected and how it will be processed, the CMS operationalizes how consent for these activities is obtained, tracked and maintained. Together, they ensure that consent is aligned with the stated purposes in the BRD and that data is processed strictly within those boundaries. This integration allows organizations to embed privacy into business processes, achieve accountability and create an auditable trail of compliance, which is critical in case of regulatory inquiries or disputes.

6. Practical Challenges & Solutions

Implementing BRD and CMS frameworks under the DPDP Act presents several practical challenges. First, organizations may face difficulties in designing consent flows that are both user-friendly and legally compliant, especially when dealing with diverse digital platforms. Second, integrating the CMS with existing organizational systems can be complex and resource-intensive. Third, tracking withdrawals of consent and ensuring corresponding deletion of personal data in real time is a complex operational requirement. To address these issues, organizations can adopt privacy by design principles, deploy automated consent dashboards and implement data mapping tools that link consent status with data processing activities. Regular audits, staff training and adoption of standardized consent management APIs can further strengthen compliance and reduce risks of inadvertent violations.

7. Conclusion

As organizations increasingly rely on personal data to drive business growth and digital innovation, compliance with the DPDP Act becomes central to sustainable operations. The integration of BRD and CMS ensures that privacy obligations are embedded in business processes and supported by robust technological systems. Although challenges such as legacy system integration, user-centric consent flows and real-time compliance may arise, these can be effectively managed through privacy by design approaches, automated dashboards and regular audits. Ultimately, organizations that invest in comprehensive compliance frameworks will not only mitigate regulatory risks but also strengthen stakeholder confidence and create a competitive advantage in an evolving digital ecosystem. The DPDP Act thus offers an opportunity for businesses to shift from a reactive approach to data protection toward a proactive, accountable and trust-building model of governance.

References:

- https://www.pwc.in/assets/pdfs/news-alert/regulatory-insights/2025/pwc_india_regulatory_insights_13_june_2025_business_requirement_document_for_consent_management_under_the_dpdp_act.pdf
- https://d38ibwa0xdgwxx.cloudfront.net/create-edition/7c2e2271-6ddd-4161-a46c-c53b8609c09d.pdf
- https://www.lexology.com/library/detail.aspx?g=5696acec-59c8-4d71-9c5b-0c1e43f86940

DISCLAIMER

ABOUT UJA

The UJA's team specializes in offering a wide range of legal solutions, ensuring comprehensive support for both businesses and individuals.

Our Comprehensive Services Include:

- Legal Advisory
- Contract Negotiation & Management
- Financial & Legal Due Diligence
- Immigration related Services
- Drafting & reviewing of legal documents, policies & Notices
- Labour Law
- Dispute Resolution & Arbitration
- Business & Operational Restructuring for M&A
- Trademark Filing & IP related advisory
- Legal Metrology & Related Services

UJA supports businesses in navigating complex regulations, global markets, and GI laws. Operating across France, Germany, Japan, Spain and more, we specialize in market entry, expansion and offering tailored solutions for growth. With over 29 years of experience and a team of 170+ experts, we have helped more than 1000 clients from SMEs to MNCs achieve their goals. Headquartered in Pune, we have offices across India - Bengaluru, Gurugram, Mumbai and International Offices in Japan, Italy and France with the representation in Germany, Spain & the UAE.

OUR TEAM

UJA
Audit • Tax • Legal • Advisory

Archana Dadhich
HOD - Corporate & Commercial Law

Archana offers a decade of experience in legal compliance business transactions, contract law, Intellectual Property Rights, licensing and other regulations such as analysis and identification of legal risks/implications. She is responsible for the entire legal processes of the firm, from deals to litigation and business transactions in M&A.

Nitin Krishnan
Senior Advisor - Legal & Strategy France

Nitin has practiced law in India, gaining experience in assisting foreign companies with India entry and regulatory matters. He has worked as a legal advisor for Business France, French Embassy in India. Alongside his legal expertise, Nitin is proficient in French which aids him in understanding French culture and handling cross-border legal issues.

Sirman Khandge
Senior Assosiate - Corporate & Comercial Law

Simran Khandge holds a bachelor's in law from Shankarrao Chavan Law College, Pune. She specialized in Competition Law, Business Law and Legal research. Over the past four years, she acquired solid experience in corporate and regulatory laws with government and private organizations.

Priya Sasanani
Senior Associate Corporate & Commercial Law

Priya Sasanani has completed her LLB from Savitribai Phule University and BCom Hons. (Entrepreneurship) from Symbiosis, Pune. She specializes in Intellectual Property laws, Commercial Laws, Legal Drafting and Legal Research. Her four years of experience comprises of working in the domain of IPR, Corporate and Regulatory laws with corporate and law firms.

Nilesh Budhiwant
Associate - Corporate and Commercial Law

Nilesh Budhiwant has completed both his Bachelor's and master's degrees in political science from Pune University. Additionally, he has earned a bachelor's in law and a master's in law with a specialization in Business Law, also from Pune University. With three years of experience in legal research, legal drafting and review, he aims to further his knowledge in Intellectual Property Law, Labor Law and Real Estate Law.