



DPDP ACT COMPLIANCE PLAYBOOK

PLAYBOOK

DPDP Act Compliance Playbook: A Practical Guide for Corporates and Startups

Introduction

As businesses increasingly rely on personal data to develop products, personalise user experiences, and improve operational efficiency, concerns regarding privacy, data security, and accountability have assumed greater significance. Against this backdrop, the Digital Personal Data Protection Act, 2023 (DPDP Act) establishes India's first comprehensive legal framework governing the processing of digital personal data, signalling a shift from fragmented sector-specific regulation to a unified privacy regime.

The DPDP Act applies to the processing of digital personal data by both public and private entities and seeks to balance innovation with the protection of individual privacy. It introduces a rights-based framework that recognises individuals as *Data Principals* while placing corresponding obligations on organisations acting as *Data Fiduciaries*. The subsequent Digital Personal Data Protection Rules, 2025 supplement the statutory framework by providing greater operational clarity on matters such as notice requirements, consent management, security safeguards, breach reporting, grievance redressal, and the responsibilities of entities processing personal data.

For many businesses, however, compliance is often perceived as a matter of updating a privacy policy or introducing an additional consent checkbox during user onboarding. In reality, the DPDP framework demands a far more comprehensive organisational approach. Privacy compliance now extends beyond legal documentation and encompasses product design, cybersecurity, vendor management, employee training, customer support, and internal governance. Every stage of the data lifecycle—from collection and processing to retention and deletion—must be supported by transparent processes and demonstrable accountability.

This shift is particularly significant for startups and growing enterprises. Unlike large corporations with dedicated legal and compliance teams, many emerging businesses operate with lean resources while processing substantial volumes of customer and employee data. Integrating privacy requirements early not only reduces future regulatory risk but also avoids expensive operational restructuring as the business

scales. Increasingly, investors, enterprise clients, and consumers also view robust data governance as an indicator of organisational maturity and trustworthiness.

This playbook provides a practical overview of the core compliance measures that start-ups should prioritise under the DPDP framework. It examines the essential components of an effective compliance programme, including obtaining valid consent, drafting transparent privacy notices, facilitating Data Principal rights, preparing for personal data breaches, and managing third-party processors through appropriate contractual safeguards through a structured compliance checklist. Rather than serving as an exhaustive legal commentary, the objective is to translate statutory obligations into practical measures that corporates and startups can incorporate into their day-to-day operations while fostering a culture of responsible data governance.

Consent: Building a Lawful Processing Framework

Consent lies at the heart of the DPDP Act and serves as one of the primary legal grounds for processing personal data. The Act departs from the long-standing practice of relying on broad, generic consent clauses embedded within lengthy privacy policies and instead requires organisations to obtain consent that is free, specific, informed, unconditional and unambiguous. Consent must be signified through

- a clear affirmative action by the Data Principal,
- ensuring that individuals retain genuine control over how their personal information is collected and used
- where transparency and accountability are integral to business operations rather than mere compliance formalities.

For corporates and startups, obtaining valid consent extends beyond incorporating a checkbox into an online registration form.

Request for consent must —

- Clearly explain the purpose of collecting personal data.
- Specify the types of data being collected.
- Outline how the information will be handled.
- Inform individuals about how they can exercise their rights.

- Keep consent requests focused and avoid mixing unrelated purposes. Example: A food delivery service should ask separately about using a customer's address for personalised ads and sharing it with partners.
- Follow the principles of the DPDP framework to ensure compliance.
- Build consumer trust by respecting user autonomy.
- Embrace transparency to maintain high user confidence.

Equally significant is the requirement that consent should remain revocable throughout the lifecycle of data processing. The DPDP Act recognises that individuals may subsequently decide that they no longer wish their personal data to be processed for a particular purpose. If consent can be provided through a mobile application with a single click, requiring users to navigate multiple webpages, submit written requests, or contact customer support merely to withdraw that consent would be inconsistent with the spirit of the legislation. Businesses should therefore integrate simple withdrawal mechanisms into their digital interfaces while simultaneously establishing internal procedures to ensure that the withdrawal is promptly reflected across all relevant systems.

- - The compliance burden with consent includes organizational governance.
- - Businesses must keep detailed records of when consent was obtained and the purposes communicated to the Data Principal.
- - Documentation should include the version of the privacy notice used and any changes or withdrawals.
- - Accurate records are crucial for proving the lawfulness of data processing.
- - Automated consent management systems and audit logs can help reduce administrative work and enhance accountability.
- - As organisations grow and handle more personal data, maintaining records is vital for compliance with relevant laws and regulations.

The DPDP framework also introduces the concept of Consent Managers, independent entities registered with the Data Protection Board that facilitate the giving, managing, reviewing, and withdrawal of consent through an interoperable platform. Although their role is expected to evolve as the regulatory ecosystem matures, organisations should remain cognizant of the possibility that consent management may increasingly become standardised across sectors. Businesses designing privacy programmes today should therefore adopt flexible consent architectures capable of integrating with future regulatory developments instead of relying upon rigid or proprietary mechanisms.

A thoughtfully crafted consent framework is a fantastic opportunity to enhance transparency and build trust. When approached positively, consent transforms from just a requirement into a foundational element of responsible data governance, paving the way for stronger connections and ethical practices.

Notice: Ensuring Transparency in Data Processing

Transparency is one of the foundational principles underpinning the DPDP Act, and the requirement to provide a clear and accessible notice is central to achieving this objective. While consent enables the lawful processing of personal data, a notice ensures that such consent is informed by giving individuals a clear understanding of how their personal information will be handled.

In other words, a privacy notice bridges the information gap between the Data Fiduciary and the Data Principal, allowing individuals to make meaningful decisions regarding their personal data rather than agreeing to processing based on incomplete or inaccessible information.

The DPDP Act, read together with the Digital Personal Data Protection Rules, 2025, requires Data Fiduciaries to provide a notice at or before the time personal data is collected. The following is essential information related to such notices:-

- Privacy notices must clearly communicate the categories of personal data collected and their purposes.
- They should outline the rights of the Data Principal under the law and how to exercise those rights.
- Effective communication is crucial; notices should not be dense legal jargon but easily understandable.
- For startups and digital products, privacy notices should enhance user experience rather than serve as mere legal disclaimers.
- Concise notices during registration, with detailed privacy policies available via hyperlink, balance transparency and usability.
- Contextual notices should inform users about additional data collection at the point of interaction.
- Privacy notices should be dynamic and updated as business models, technologies, or data practices change.
- Organisations must transparently communicate any material changes in data processing to keep users informed.
- Balancing legal accuracy with readability.

- Privacy notices should avoid excessive technical terminology and instead use plain, straightforward language that an average user can understand. This is particularly relevant in sectors such as fintech, health-tech, ed-tech, and e-commerce, where individuals routinely share significant volumes of personal data without fully appreciating the implications of such processing.
- Clear headings, concise explanations, and layered notices can significantly improve user comprehension while simultaneously strengthening organisational compliance.

Ultimately, an effective privacy notice serves purposes that extend beyond satisfying statutory requirements. It demonstrates an organisation's commitment to openness, accountability, and responsible data governance. In an increasingly competitive digital marketplace, businesses that communicate transparently about their data practices are more likely to foster consumer trust, reduce misunderstandings regarding data use, and strengthen their overall compliance posture under the DPDP framework. Rather than viewing privacy notices as administrative formalities, organisations should regard them as one of the most visible manifestations of their commitment to respecting the privacy rights of individuals.

Data Principal Rights: Facilitating Individual Control over Personal Data

A defining feature of the DPDP Act is its recognition of individuals as active participants in the data ecosystem rather than passive subjects of data collection. By conferring a set of enforceable rights upon Data Principals, the Act seeks to promote transparency, accountability, and individual autonomy in relation to personal data. These rights impose corresponding obligations on Data Fiduciaries, requiring organisations to establish systems and processes that enable individuals to meaningfully exercise control over how their personal information is processed. Compliance, therefore, extends beyond drafting privacy policies and requires businesses to operationalise these rights through effective governance mechanisms. The Act provides Data Principals with several important rights:

- Right to obtain information about personal data processing
- Right to seek correction, completion, updating, or erasure of personal data
- Right to withdraw consent
- Right to nominate another individual to exercise rights in certain situations
- Right to access an effective grievance redressal mechanism.

Collectively, these rights are intended to ensure that individuals remain informed about the use of their personal data and retain the ability to challenge or modify processing activities that affect them.

Right under the DPDP Act	Business Obligation	Practical Compliance Measure
Right to Access Information	Provide information regarding the processing of personal data	Establish a dedicated request portal or support channel for information requests
Right to Correction and Erasure	Correct inaccurate information or erase personal data where legally permissible	Implement standardised correction and deletion workflows within internal systems
Right to Withdraw Consent	Stop processing personal data where consent forms the legal basis	Enable simple and accessible consent withdrawal mechanisms across digital platforms
Right to Grievance Redressal	Provide an effective mechanism for resolving complaints	Appoint a Grievance Officer and establish defined response timelines
Right to Nominate	Facilitate nomination in accordance with the Act and applicable Rules	Incorporate nomination functionality within user account management systems, where relevant

While these rights appear straightforward in principle, their implementation often presents practical challenges. Rights implementation must include the following steps –

- Verify the identity of individuals submitting requests to protect personal data.
- Log and assign requests to the appropriate team after verification.
- Process requests within set timelines.
- Keep detailed records of requests, actions, and communications for consistency and compliance.
- Consider automation to enhance efficiency and minimise human error as request volumes increase.
- User-friendly dashboards that allow individuals to update personal information, change communication preferences, or submit data requests ease administrative tasks and improve user experience.

- It's also vital for customer support teams to be well-trained, as they are often the first point of contact for those exercising their rights under the Act.

Startups and small businesses may find the operational aspects of rights management particularly demanding due to limited financial and human resources. Nevertheless, embedding these processes early in the business lifecycle often proves more cost-effective than attempting to redesign internal systems after operations have expanded.

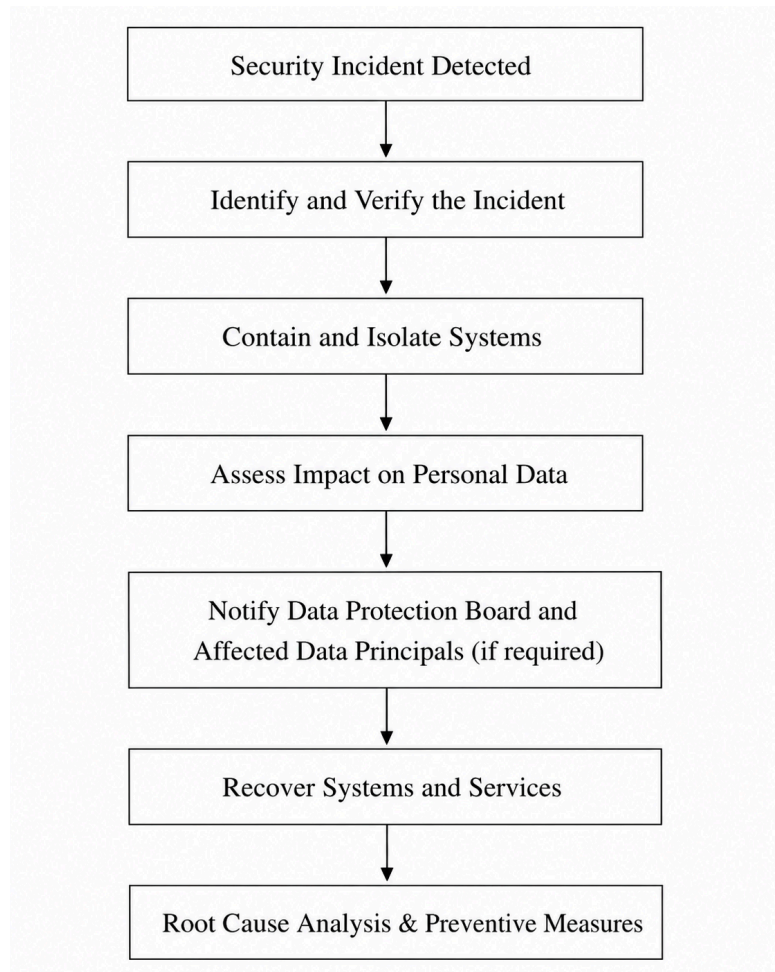
Ultimately, respecting Data Principal rights is fundamental to establishing trust within the digital economy. Organisations that respond promptly, communicate transparently, and maintain well-documented procedures demonstrate that privacy is embedded within their governance framework rather than treated as a reactive compliance obligation. As regulatory expectations continue to evolve, businesses that invest in robust rights management mechanisms will be better positioned to meet both legal requirements and growing consumer expectations regarding responsible data handling.

Breach Response: Preparing for Personal Data Breaches

Despite significant advances in cybersecurity technologies, no organisation is entirely immune from security incidents. Cyberattacks, accidental disclosures, insider threats, ransomware attacks, and system failures continue to expose organisations to the risk of unauthorised access, loss, alteration, or disclosure of personal data. Recognising this reality, the DPDP Act and the Digital Personal Data Protection Rules, 2025 require Data Fiduciaries to adopt appropriate technical and organisational security measures and establish procedures for responding effectively to personal data breaches. Breach preparedness is not merely a cybersecurity concern but an essential component of regulatory compliance and corporate governance.

A personal data breach can have far-reaching consequences beyond immediate operational disruption. It may expose individuals to financial fraud, identity theft, reputational harm, or unauthorised surveillance, while simultaneously undermining consumer confidence in the affected organisation. Businesses may also face regulatory action, financial penalties, contractual liabilities, and reputational damage arising from inadequate security safeguards or delayed responses. Accordingly, organisations should establish a structured incident response framework that clearly defines responsibilities, communication channels, escalation procedures, and reporting obligations before an incident occurs.

Figure 1. Personal Data Breach Response Workflow under the DPDP Compliance Framework



As illustrated above, responding to a personal data breach requires a systematic sequence of actions rather than isolated technical interventions. The process begins with identifying and verifying whether a security incident has occurred and determining whether personal data has been compromised. Once confirmed, the immediate priority should be to contain the incident by isolating affected systems, preventing further unauthorised access, and preserving evidence necessary for forensic investigation. Organisations should then assess the scope of the breach by identifying the categories of personal data affected, the number of Data Principals involved, the likely consequences for affected individuals, and the underlying cause of the incident.

Following this assessment, organisations must comply with the notification requirements prescribed under the DPDP framework. Where applicable, personal data breaches should be reported to the relevant regulatory authority and affected Data Principals within the prescribed timelines and in the manner specified by the Rules. Notifications should communicate the nature of the breach, the categories of data involved, the potential risks arising from the incident, and the measures being undertaken to mitigate its

impact. Timely and transparent communication enables affected individuals to take appropriate protective measures while demonstrating the organization's commitment to accountability and responsible data governance.

The final stage of incident response extends beyond restoring affected systems. Organizations should undertake a comprehensive post-incident review to identify weaknesses in existing security controls, evaluate the effectiveness of their response procedures, and implement corrective measures to reduce the likelihood of recurrence. This may involve updating internal policies, strengthening technical safeguards, revising vendor management practices, conducting employee training, or performing additional cybersecurity assessments. Maintaining detailed documentation throughout the incident lifecycle is equally important, as it provides evidence of compliance and supports future audits, investigations, or litigation.

Ultimately, an effective breach response framework is built long before a security incident occurs. Companies that regularly test their incident response plans through tabletop exercises, maintain clear reporting structures, and cultivate a culture of cybersecurity awareness are better equipped to respond swiftly when breaches arise. In the evolving landscape of digital regulation, preparedness is no longer optional but an essential element of responsible data governance under the DPDP framework.

Data Processing Agreements: Managing Third-Party Compliance

Modern businesses rarely process personal data entirely through their own internal infrastructure. Cloud service providers, payment gateways, payroll processors, customer relationship management platforms, software vendors, analytics providers, and outsourced customer support services routinely process personal data on behalf of businesses. While outsourcing these functions may improve operational efficiency and reduce costs, it also introduces additional compliance risks. The DPDP Act places the primary responsibility for lawful processing on the Data Fiduciary, meaning that organizations cannot avoid liability merely because personal data is processed by a third party.

This makes effective vendor management an integral component of any privacy compliance programme. Before engaging a third-party processor, businesses should undertake appropriate due diligence to assess the vendor's technical capabilities, cybersecurity practices, internal governance mechanisms, and overall ability to comply with applicable data protection obligations. The objective is not only to evaluate

commercial suitability but also to determine whether the processor can maintain an appropriate standard of security and confidentiality throughout the data processing lifecycle. Periodic reassessment is equally important, particularly where vendors process large volumes of personal data or provide critical digital infrastructure.

A well-drafted Data Processing Agreement (DPA) serves as the principal contractual mechanism for allocating responsibilities between the Data Fiduciary and the processor. Such agreements should clearly define the nature and purpose of processing, the categories of personal data involved, the duration of processing, the security measures to be implemented, confidentiality obligations, breach notification procedures, audit rights, and the obligations applicable upon termination of the contractual relationship. Clearly allocating these responsibilities reduces uncertainty during routine operations and enables a coordinated response if security incidents occur.

Businesses should also recognise that vendor compliance is an ongoing responsibility rather than a one-time contractual exercise. Technology providers frequently introduce new features, migrate infrastructure, appoint sub-processors, or expand their processing activities over time. Consequently, organisations should periodically review vendor contracts, monitor compliance certifications where applicable, and reassess whether existing safeguards remain appropriate in light of evolving business operations and regulatory requirements. Maintaining an up-to-date register of third-party processors and the categories of personal data shared with each vendor can further strengthen governance and simplify incident response if a breach occurs.

For startups and small enterprises, standardized contractual templates and structured vendor onboarding procedures can significantly reduce compliance risks while avoiding unnecessary administrative complexity. Larger organizations, on the other hand, may benefit from adopting risk-based vendor classification models, whereby processors handling sensitive or high-volume personal data are subjected to enhanced contractual obligations and more frequent compliance reviews. Regardless of organizational size, integrating contractual safeguards with broader information security and governance frameworks is essential to ensuring that third-party relationships do not become weak links in an otherwise robust privacy programme.

Ultimately, effective data protection extends beyond the organizational boundary. As businesses become increasingly dependent on interconnected digital ecosystems, robust Data Processing Agreements and proactive vendor oversight are indispensable tools for ensuring accountability across the entire chain of data processing. Organizations that carefully select, contract with, and monitor their processors are better

positioned to meet their obligations under the DPDP framework while preserving the trust of customers, employees, and other stakeholders.

DPDP Readiness Checklist: Assessing Organisational Preparedness

Compliance with the DPDP Act should not be viewed as a one-time exercise completed through the adoption of a privacy policy or the execution of contractual documents. Instead, it requires organisations to establish an integrated governance framework that combines legal compliance, operational procedures, technical safeguards, and employee awareness. Conducting periodic internal assessments allows businesses to identify compliance gaps, monitor evolving regulatory obligations, and ensure that privacy practices remain aligned with changes in business operations and technology. For startups, such assessments also facilitate scalable growth by embedding privacy considerations into products and processes from the outset rather than attempting costly modifications at a later stage.

The following checklist provides a practical starting point for organizations seeking to evaluate their readiness under the DPDP framework. While the precise measures adopted will vary depending on the nature and scale of data processing activities, these foundational elements are relevant across most industries.

Compliance Area	Readiness Status
Personal data inventory and data mapping completed	☐
Privacy notice reviewed and updated	☐
Consent collection and withdrawal mechanisms implemented	☐
Internal process for handling Data Principal requests established	☐
Grievance Redressal mechanism and responsible officer designated	☐
Data Processing Agreements executed with relevant vendors	☐
Appropriate technical and organisational security measures implemented	☐
Personal data breach response plan documented and tested	☐

Employee awareness and privacy training conducted ☐

Data retention and deletion policy implemented ☐

Periodic compliance reviews and internal audits scheduled ☐

Although this checklist provides a useful benchmark, organisations should recognise that compliance is a continuous process rather than a fixed destination. As business models evolve, new technologies are adopted, and regulatory expectations continue to develop, privacy programmes should be reviewed and refined accordingly. Regular policy reviews, employee training, vendor assessments, and incident response exercises help ensure that compliance remains effective in practice rather than existing merely as documented policy. Ultimately, businesses and start-ups that adopt a proactive and risk-based approach to privacy governance are better positioned to satisfy regulatory expectations while fostering long-term trust among customers, employees, and business partners.

Conclusion

The Digital Personal Data Protection Act, 2023, together with the Digital Personal Data Protection Rules, 2025, marks a significant milestone in India's evolving digital regulatory landscape. By establishing a comprehensive framework for the collection, processing, storage, and protection of digital personal data, the legislation seeks to balance the interests of innovation and economic growth with the fundamental need to safeguard individual privacy. For businesses, this represents a transition from fragmented privacy practices to a structured model of accountability in which compliance must be embedded across organisational functions rather than confined to legal documentation.

As this playbook demonstrates, effective compliance extends well beyond obtaining consent or publishing a privacy policy. Organisations must adopt transparent notice practices, establish reliable mechanisms for facilitating Data Principal rights, prepare for personal data breaches through structured incident response plans, and ensure that third-party processors are subject to appropriate contractual and operational safeguards. Equally important is developing an internal culture of privacy, supported by employee awareness, regular compliance assessments, and continuous improvement of governance practices. These measures collectively strengthen an organisation's ability to demonstrate accountability while reducing operational and regulatory risks.

For corporates and startups alike, the DPDP framework should be viewed not merely as a statutory obligation but as an opportunity to strengthen consumer trust in an increasingly data-driven economy. Businesses that integrate privacy into product design, corporate governance, and everyday decision-making are likely to enjoy long-term advantages extending beyond legal compliance, including enhanced customer confidence, stronger investor assurance, and improved resilience against emerging cyber risks. As India's data protection regime continues to mature through evolving regulatory guidance and enforcement practices, organizations that adopt a proactive and privacy-centric approach today will be better equipped to navigate the challenges and opportunities of tomorrow's digital ecosystem.



Fractional General Council

A-9, Block A, Sector 68, Noida,
Basi Bahuddin Nagar, Uttar Pradesh 201309

www.fracgc.in

contact@fracgc.in

[+91 83770 09673](tel:+918377009673)
