Understanding India's Digital Personal Data Protection (DPDP) Act and Steps To Achieving Continuous Compliance

Introduction

India's Digital Personal Data Protection (DPDP) Act, enacted on August 9, 2023, marks a significant milestone in the governance of personal data collection and processing within the country. The Act establishes a framework that empowers individuals, referred to as Data Principals, to have comprehensive rights concerning their personal data. This report delves into the rights of Data Principals, the responsibilities of organizations, additional measures for compliance, penalties for noncompliance, and the current status of the DPDP Act. The Act is widely viewed as a foundational step toward establishing robust data privacy regulations in India, aligning with global standards.

Rights of Data Principals

The DPDP Act grants several essential rights to Data Principals, fostering transparency and control over personal data. These rights include:

RIGHT TO KNOW

Data Principals have the right to be informed about the personal data being collected about them. They must be made aware of the purpose of data collection and the third parties with whom their data may be shared. This right ensures that individuals are not kept in the dark about how their data is utilized.

RIGHT TO ACCESS

Individuals have the right to access their personal data that is being processed by an organization. This includes the ability to request details about the nature of the data, its origin, and how it is being processed, thereby allowing Data Principals to review their information and ensure its accuracy.

RIGHT TO CORRECT OR DELETE

Data Principals are empowered to correct any inaccuracies in their personal data. They also have the right to delete their personal data under specific circumstances. This right emphasizes the importance of data accuracy and allows individuals to maintain control over their personal information.

RIGHT TO OBJECT

Individuals can object to the processing of their personal data in certain situations. This right allows Data Principals to opt out of data processing that they deem unnecessary or intrusive, promoting user autonomy over personal data.

RIGHT TO DATA PORTABILITY

Data Principals have the right to port their personal data to another organization, allowing for greater flexibility and choice when switching services. This right fosters a competitive environment among service providers, encouraging better practices in data handling.

RIGHT TO FILE A COMPLAINT

If individuals believe that their personal data has been processed in violation of the DPDP Act, they have the right to file a complaint with the Data Protection Board (DPB). This provision reinforces the accountability of organizations and provides Data Principals with a channel for redressal.

Responsibilities Organizations

The DPDP Act also outlines the responsibilities of organizations processing personal data. Key obligations include:

OBTAIN CONSENT

Organizations must obtain explicit consent from individuals before processing their personal data unless specific exemptions apply. This requirement ensures that individuals remain informed and consenting participants in data processing activities.

RESPOND TO REQUESTS

Organizations are required to respond to individuals' requests for access, correction, deletion, and objection within a reasonable timeframe. This obligation promotes timely communication and compliance with Data Principals' rights.

DATA PROTECTION MEASURES

Organizations must take appropriate technical and organizational measures to protect personal data from unauthorized access, use, disclosure, alteration, or destruction. This includes implementing cybersecurity measures and privacy protocols to safeguard sensitive information.

PURPOSE LIMITATION

Organizations are obliged to use personal data solely for the purpose for which it was initially collected. This principle reinforces the idea that consent is not a blanket authorization and that individuals should have clarity on how their information is utilized.

REPORT DATA BREACHES

In the event of a data breach, organizations must report the incident to the DPB within 72 hours of becoming aware of the breach. This requirement ensures that authorities and affected individuals can take prompt action to mitigate potential harm.

Additional Responsibilities for Organizations

To enhance accountability and compliance, organizations can consider the following practices:

DATA PROCESSING ASSESSMENT

Organizations should conduct a thorough assessment of their data processing activities to identify areas that require modification to comply with DPDP Act requirements. This proactive approach aids in aligning practices with legal obligations.

APPOINT A DPO

Organizations processing personal data on a large scale are required to appoint a Data Protection Officer. The DPO is responsible for overseeing compliance with the DPDP Act and serving as a point of contact for Data Principals and regulatory authorities.

DEVELOP A DATA PROTECTION POLICY

Establishing a clear data protection policy signifies an organization's commitment to protecting personal data. This policy should delineate data management practices and compliance measures.

CONDUCT INDEPENDENT AUDITS

Periodic audits by independent third parties can help organizations ensure ongoing compliance with the DPDP Act. Such audits provide organizations with insights into compliance gaps and areas for improvement.

Penalties for Noncompliance

The DPDP Act establishes strict penalties for violations of its provisions. Organizations that fail to implement necessary information security measures or violate Data Principals' rights may face fines of up to 250 crore INR (approximately $30 million). This penalty structure is notably less severe than earlier proposals, which aimed to impose fines of up to 500 crore INR (approximately $61 million).

The reduction in penalty amounts reflects a balanced approach to enforcement, aiming to encourage compliance while providing organizations with a manageable framework to operate within.

Frequently Asked Questions

Has the Personal Data Protection Act been passed in India?	What is a data subject in the Digital Personal Data Protection Act?	Is data privacy a human right in India?
Yes, the Digital Personal Data Protection Act was passed on August 9, 2023, establishing a legal framework for personal data protection.	The Act uses the term "Data Principals" to refer to individuals whose personal data is processed, including provisions for minors under the guardianship of their parents or lawful guardians.	While the Indian Constitution does not explicitly enshrine the right to privacy, the Supreme Court's 2017 ruling recognized it as a fundamental right under Articles 14, 19, and 21, affirming data privacy's significance.

The DPDP Act (DPDPA) can put a heavy burden on organizations in terms of manual effort and resources required to make sure they are compliant, especially in lieu of the Rights of Data Principals. Compliance is critical on two fronts, building trust in doing business across India for both Principals and Partner, but also in avoiding fines.

Continuous DPDPA Compliance with Minimal Effort and Resources

Achieving compliance easily has been impossible to achieve because various stakeholders must manually cobble together data, which takes a lot of time and is resource intensive. Even most current solutions are focused on delivering pieces of information required to achieve compliance versus a comprehensive approach, requiring different teams to access different solutions and manually stitch results together. Often any sort of visibility or assessment of risk is point-in-time, meaning it is out of date quickly, especially when using cloud infrastructure of modern data warehouse solutions with data-in-motion. Continuous compliance seems even more unattainable due to lack of accurate and automated remediation of data risks as they are discovered in real-time. What if I could attain all the visibility, risk assessment, reporting and even remediate exposed data that is at risk in hours versus days or weeks?

Borneo's Data Risk Remediation (DRR) Platform for Continuous DPDP Act Compliance

Borneo provides the industry's first Data Risk Remediation (DRR) platform built by data practitioners for practitioners to eliminate risks in real-time associated with exposed sensitive data. This includes proactive and accurate remediation of data risks that could lead to leaked data and breaches, while also delivering continuous compliance for simplifying data privacy and protection regulations such as India's Digital Personal Data Protection (DPDP) Act. Below is an outline of how Borneo.io supports organizations in achieving DPDP compliance:

DATA DISCOVERY AND CLASSIFICATION	• Automated Data Mapping: Borneo.io helps organizations discover and map all types of personal data across their systems. This provides a comprehensive view of what data is held, where it is stored, and how it flows within the organization. • Data Classification Tools: The platform enables classification of data based on sensitivity and compliance requirements, ensuring that organizations understand the nature of the data they handle.
CONSENT MANAGEMENT	• Dynamic Consent Collection: Borneo.io allows organizations to collect and manage consent from Data Principals when processing their personal data. This includes customizable consent forms and clear opt-in/out options. • Consent Records: The platform maintains a record of consent and preferences, facilitating easy access and updating per Data Principal requests.
RIGHTS MANAGEMENT	• Facilitating Data Access Requests: Borneo.io streamlines the process for Data Principals to request access to their personal data. The platform automates the gathering and sharing of relevant data with users, ensuring compliance with the access rights outlined in the DPDP Act. • Data Correction and Deletion Features: The platform provides tools for managing requests for data correction and deletion, allowing organizations to respond quickly and efficiently to these requests.
DATA PROCESSING TRANSPARENCY	• Privacy Policies and Notices: Borneo.io assists organizations in creating clear and compliant privacy policies and notices that inform Data Principals about their data processing activities, purposes, and third-party sharing.

	• Real-time Activity Logs: The platform provides detailed logs of data processing activities, which organizations can use to demonstrate transparency and compliance.
SECURITY MEASURES	• Data Protection Protocols: Borneo.io offers features for encrypting and anonymizing personal data, ensuring that sensitive information is safeguarded against unauthorized access and breaches. • Incident Management: The platform includes tools for managing data breaches, allowing users to document and report incidents promptly, thus meeting the 72-hour notification requirement stipulated by the DPDP Act.
AUDIT AND COMPLIANCE REPORTING	• Automated Compliance Assessments: Organizations can conduct regular assessments using Borneo.io to ensure their practices align with the requirements of the DPDP Act. • Audit Trails: The platform maintains detailed logs of all data handling activities, making it easy for organizations to produce audit trails for compliance reviews and inspections.
STAFF TRAINING AND AWARENESS	• Training Modules: Borneo.io provides training resources to educate staff on data protection best practices, the significance of compliance, and their roles in maintaining data security and privacy. • Ongoing Support: The platform may offer ongoing support and resources to keep businesses updated on changes in legal requirements and data protection practices.
SCALABILITY AND INTEGRATION	• Integration Capabilities: Borneo.io is designed to integrate easily with existing systems, allowing organizations to enforce compliance without needing to overhaul their current data infrastructure. • Scalability: The platform can scale with an organization's needs, accommodating growth in data processing activities while ensuring continued compliance.

Conclusions

The Digital Personal Data Protection Act marks a pivotal shift in personal data governance in India, establishing clear rights for Data Principals and outlining the responsibilities of organizations. By fostering transparency, accountability, and individual empowerment, the DPDP Act enhances data protection and privacy, reflecting the growing global emphasis on safeguarding personal information in the digital age. As the country implements these provisions, ongoing awareness, compliance efforts, and stakeholder engagement will be vital to realize the full potential of this transformative legislation.

Borneo's Data Risk Remediation Platform provides a unified data security solution focused on delivering continuous remediation for organizations seeking to comply with the DPDP Act. By enabling organizations to simplify and automate the tasks for meeting the requirements of regulatory agencies with high-degree of accuracy, Borneo enables organizations to automatically take the necessary steps to protect sensitive data. Through Borneo's ability to remediate data risks in real-time, organizations are able to achieve continuous compliance, ultimately fostering trust between organizations and Data Principals.

To learn more about how Borneo can eliminate your data risks and help you streamline compliance with the DPDP Act as your business grows and evolves, please contact us at info@borneo.io or visit our website at https://borneo.io.

