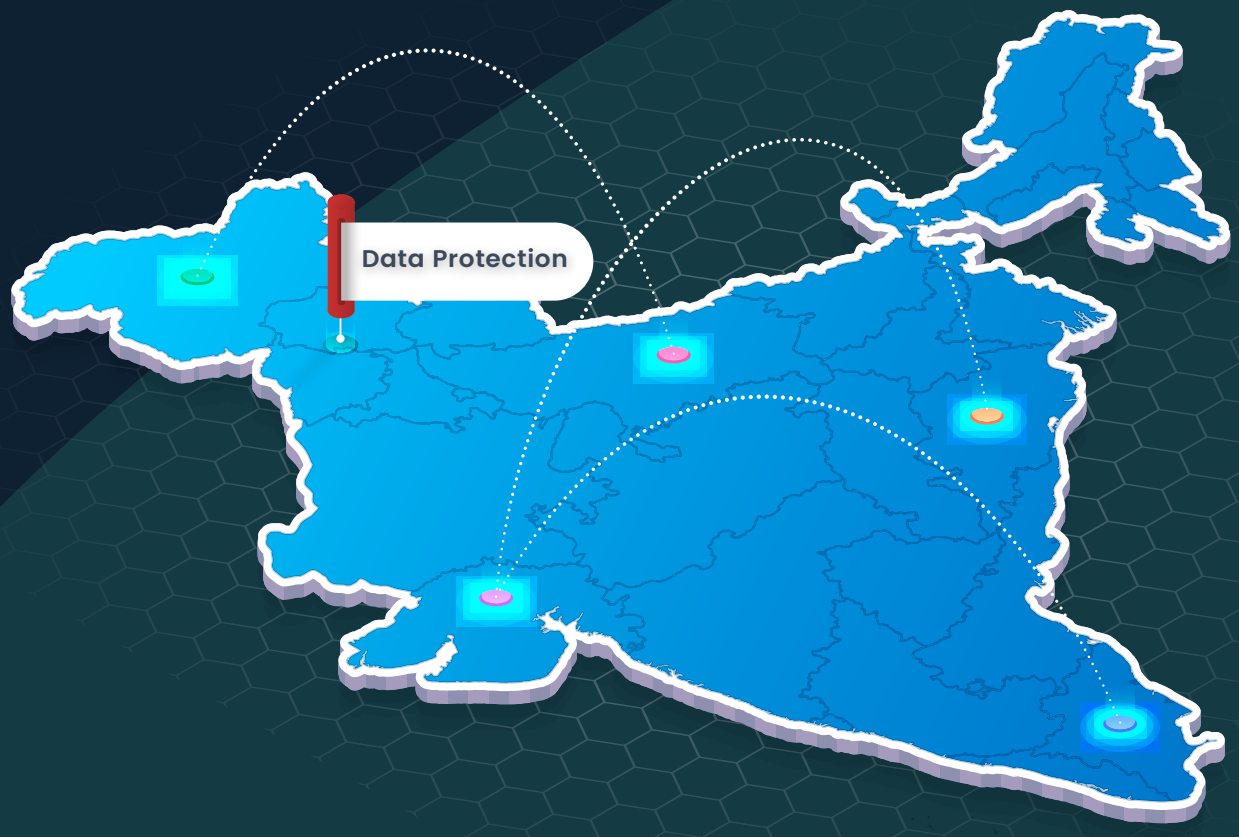
Scrut Automation

Navigating India's Digital Personal Data Protection Bill, 2023: **A Comprehensive Guide**



Scrut Automation

Contents

Introduction

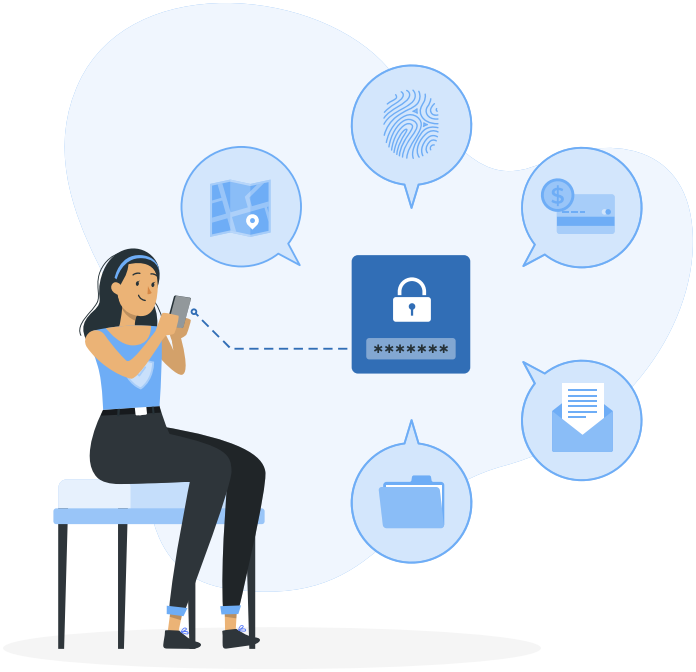
Data protection has emerged as a top concern, particularly in a country as technologically diverse as India. The proliferation of digital platforms, online transactions, and interconnected devices has resulted in an unprecedented generation and flow of personal data.

The significance of data protection lies in safeguarding individuals' privacy, ensuring the secure management of sensitive information, and fostering trust in the digital ecosystem. Recognizing the urgency of these challenges, India has taken a significant step forward with the introduction of the Digital Personal Data Protection Bill, 2023.

This landmark legislation aims to establish a comprehensive framework for the collection, storage, processing, and transfer of personal data by entities, both governmental and private, operating within the boundaries of India. It balances the needs of innovation and economic growth with the aim of ensuring individuals' rights and privacy.

By addressing issues such as consent, data localization, and enforcement mechanisms, the bill reflects India's commitment to creating a digital environment that is both technologically advanced and ethically responsible, highlighting the pivotal role that data protection plays in shaping the nation's digital future.

In this ebook, we will walk you through everything you need to know about the bill – understand what it entails, how it can affect you as an individual and how it can affect your business. We will also help you prepare for the bill by listing ways to help you stay compliant and adapt well to this new and important regulation.



Chapter 1: What you should know about the DPDP Bill, 2023

Approved by both houses of Parliament on August 9, 2023, the Digital Personal Data Protection Bill (DPDPB) of 2023 stands as India's first comprehensive privacy legislation.

Crafted to oversee the processing of digital personal data, the DPDP Bill aptly recognizes the dual need for safeguarding individuals' personal information rights and accommodating the legitimate data processing needs of organizations.

At its core, the bill aims to establish a comprehensive and cohesive legal framework governing the collection, storage, processing, and cross-border movement of personal data. This framework applies to both governmental and private entities operating within India's jurisdiction.

One notable aspect of the bill is its stipulation of fines for non-compliance with pivotal requirements such as obtaining explicit consent for data processing, underscoring the critical importance for organizations handling personal data to thoroughly comprehend and adhere to its provisions.

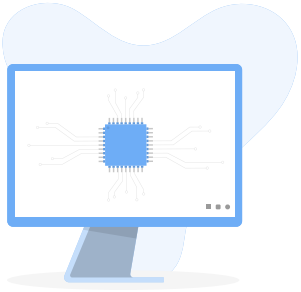
Scope and structure of the bill

The Digital Personal Data Protection Bill (DPDPB) of 2023 has a clear focus on its coverage. It defines personal data as information that can directly or indirectly identify an individual. This law applies to the handling of personal data within India, whether it's in a digital format or has been digitized from physical records.

Furthermore, the DPDP Bill extends its jurisdiction beyond India's borders, especially when digital personal data is used to offer goods or services to individuals within the country. However, it's important to note that the bill does not apply to personal data that individuals use for their own personal or domestic purposes, or to data that is already publicly available.

The DPDP Bill is thoughtfully structured into six chapters, containing 33 sections, and includes a schedule outlining penalties for non-compliance. Within this legal framework, several key stakeholders come into play.

Stakeholders listed in the bill



Data processor

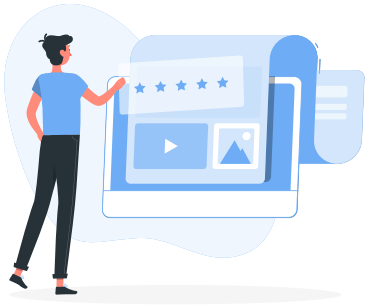
Any individual handling personal data on behalf of a data fiduciary.

Appellate tribunal (Telecom Disputes Settlement)

This This tribunal is responsible for addressing appeals and grievances concerning orders or directives issued by the Data Protection Board of India.

Data fiduciary

"Person" (which includes organizations and associations) responsible for deciding why and how personal data is processed. Some data fiduciaries might be classified as "significant data fiduciaries" depending on the kind of data they handle.



Consent managers

Individuals authorized by data principals to oversee, assess, and retract consent using a platform that is accessible, transparent, and interoperable. This platform is registered with the Board.

Data Protection Officer (DPO)

A person designated by a significant data fiduciary to carry out tasks outlined in the Bill.

Regulatory body - the Data Protection Board of India

The main regulatory authority in charge of implementing the Bill.

Provisions of the Bill

The DPDP Bill extends its protective umbrella over all forms of online data and offline data that has been digitized within India. This comprehensive coverage ensures the safeguarding of personal information. Here are its provisions:

Government Oversight: A Data Protection Board, established by the Union government, will hold authority over personal data affairs. Its primary functions involve enforcing compliance and levying penalties. The government will wield influence over the board's composition, terms of service, and overall law implementation.

Data Storage: Distinct from previous legislations, the draft bill does not impose an exclusive data storage requirement within India. Nevertheless, it restricts cross-border data transfers to countries authorized by the Indian government.

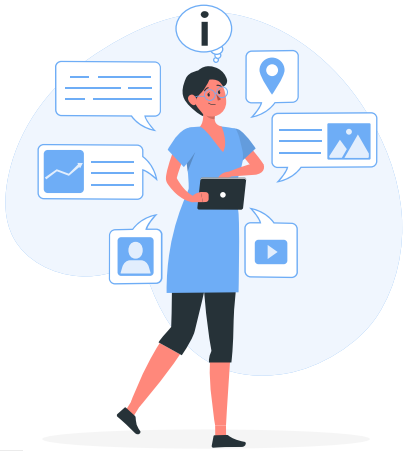
Monetary Sanctions: The draft bill introduces exclusively monetary penalties for breaches or non-compliance, ranging from INR 50 crore to INR 250 crore. Notably, a cap of INR 500 crore is set for significant data breaches.

Data Pertaining to Minors: The bill mandates parental consent for individuals below 18 years of age. However, concerns linger about the differentiation of consent between toddlers and adolescents, the potential impact on personal development, and potential violations of the Rights of the Child.

Data Collection: The draft eliminates specific constraints on data collection, allowing data fiduciaries to gather personal data with the consent of the data principal, while ensuring transparency regarding the purpose of data collection.

Government Exemptions: Government bodies can be exempted from regulations for reasons encompassing sovereignty, security, foreign relations, and public order, though specific exemption criteria are absent.

Limited Information Requirements: The draft streamlines information provision to data principals, focusing on personal data sought and the purpose of data processing. This streamlined approach excludes extensive rights, grievance mechanisms, retention periods, and data sources.



Notable Omissions:

Data Portability: This right grants data principals the ability to access and analyze their personal data in a structured format, allowing them to select platforms for data sharing and minimizing the need for re-submission of all personal data when transitioning platforms.

Foregone Information Right: The absence of this right creates ambiguity between the general right to erasure and the right to be forgotten. This may potentially undermine the freedom of speech and expression for others.

Chapter 2: Rights and Obligations under the Bill

The essence of the DPDP Bill revolves around safeguarding individual privacy within the digital era. It covers any information that can uniquely identify a person, regardless of whether this data was gathered online or offline and then converted into a digital format.

What's noteworthy is that the DPDP Bill reaches beyond the borders of India. This extension occurs specifically when digital personal data processing involves profiling or providing goods and services to individuals within India.

To put it simply, any organization worldwide that deals with the personal data of Indian citizens is obligated to follow the rules outlined in the bill.

There are various rights and obligations reserved for the stakeholders listed in the Bill. We detail them in this chapter.

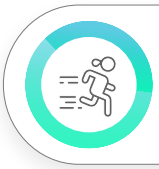
Individual Rights (Data Principals)

The right to receive information regarding their personal data

01

The right to rectify and erase their personal data

02



The right to pursue grievance resolution

03

The right to designate a third party to act on their behalf

04

Note: Data principals must adhere to relevant laws while exercising their rights as per the Bill. Failure to comply may lead to penalties of up to INR 10,000.

Data Fiduciary and Data Processor

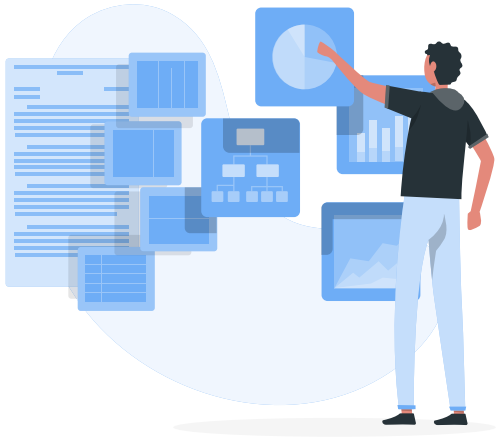
Compliance Obligations: Organizations are obliged to fulfill their duties outlined in the Bill, regardless of any agreements or non-compliance by data principals. They must ensure that personal data is accurate and complete for decision-making and disclosures, and must establish appropriate technical and organizational measures for compliance.

Notification: Data principals should receive notices detailing the personal data being processed, the purpose of processing, avenues to exercise their rights, and contact details for reaching the Board. This applies to both future and previously collected data, before the law's enactment. The notice must be provided in English or one of the 22 scheduled languages, based on the data principal's preference.

Sharing Information: Upon request from a data principal, data fiduciaries must furnish information about other data fiduciaries and data processors.

Consent: Consent should be given freely, be specific, informed, unambiguous, and accompanied by clear affirmative action for a specified purpose.

Data Handling: Data fiduciaries must ensure precise and complete processing of data, limiting it to defined purposes. Data should be deleted once the purpose is fulfilled, except if required by another law. Data fiduciaries can engage data processors only through valid contracts. Data belonging to minors and individuals with disabilities can only be processed with verified parental/guardian consent. Certain forms of processing, such as tracking, behavioral monitoring, and targeted advertising aimed at minors, are prohibited.



Breach Notification: In the event of a data breach, both the Board and affected data principals must be informed.

Significant Data Fiduciary: Entities falling into this category must appoint an India-based Data Protection Officer (DPO) and take additional measures, including Data Protection Impact Assessment and periodic data audits by an independent data auditor.

Transfer of Personal Data Outside India

The Bill permits the unrestricted transfer of personal data outside India, except to countries specifically restricted by the Central Government. Moreover, the Bill takes into account and retains provisions related to other Indian laws that might influence international data transfers.

Chapter 3: Enforcement and Penalties for Non-Compliance

The DPDP Bill is more than a set of regulations. It serves as a robust framework for safeguarding the confidentiality and privacy of personal data.

To accomplish this goal, the DPDP Bill establishes the Data Protection Board (DPB) as a pivotal entity. The DPB is entrusted with the responsibility of ensuring compliance with the bill's provisions.

However, the responsibility does not rest solely with the DPB. The bill also emphasizes the participatory role of individuals in upholding their data rights. Equipped with the power to voice grievances and seek redress, individuals are integral to the enforcement mechanism. Their active engagement reinforces the reach and efficacy of the DPDP Bill.

Role of the Data Protection Board in enforcing regulations

The DPDP Bill necessitates the formation of a Data Protection Board (DPB), which will consist of government-appointed members. The DPB's primary responsibilities encompass scrutinizing complaints, conducting investigations into data breaches, and determining penalties based on factors such as the gravity of the breach, its duration, and the frequency of recurrence.

Here's a look at its main functions:

Adjudicating Complaints and Imposing Penalties: Should the Board receive a complaint from a user, a reference from the government, or a court directive related to a breach committed by a Data Fiduciary or a Consent Manager, whether in fulfilling their obligations or respecting user rights, the Board holds the authority to investigate the breach and levy penalties as necessary.

Addressing Personal Data Breaches: In situations where a breach of personal data occurs, the Board is empowered to direct the Data Fiduciary to undertake immediate corrective actions. The Board is also entrusted with the responsibility to scrutinize the breach, and if warranted, impose penalties.

Issuing Authoritative Directions: The Board is vested with the ability to issue directions, ensuring that the concerned parties are given a fair chance to present their perspectives. This process includes recording the Board's rationale in written form. Moreover, the Board holds the authority to modify, suspend, withdraw, or revoke any previously issued direction as deemed necessary.

Penalties and consequences for non-compliance

1

Failure to Prevent Personal Data Breach:
Penalties of up to INR 250 crore (approximately USD 30 million) may be imposed for failing to avert a personal data breach.

2

Failure to Notify Breach to the Board and Data Principals:
A penalty of up to INR 200 crore can be levied for not informing both the Board and data principals about a breach.

3

Non-Fulfillment of Obligations in Processing Children's Data:
Non-compliance in meeting obligations while processing children's data may result in penalties of up to INR 200 crore.

4

Non-Fulfillment of Obligations by Significant Data Fiduciary:
Penalties of up to INR 150 crore can be imposed for failing to fulfill obligations by a significant data fiduciary.

5

Breach of Voluntary Undertaking to the Board:
Breach of any voluntary commitment made to the Board carries a penalty to the extent applicable for the breach.

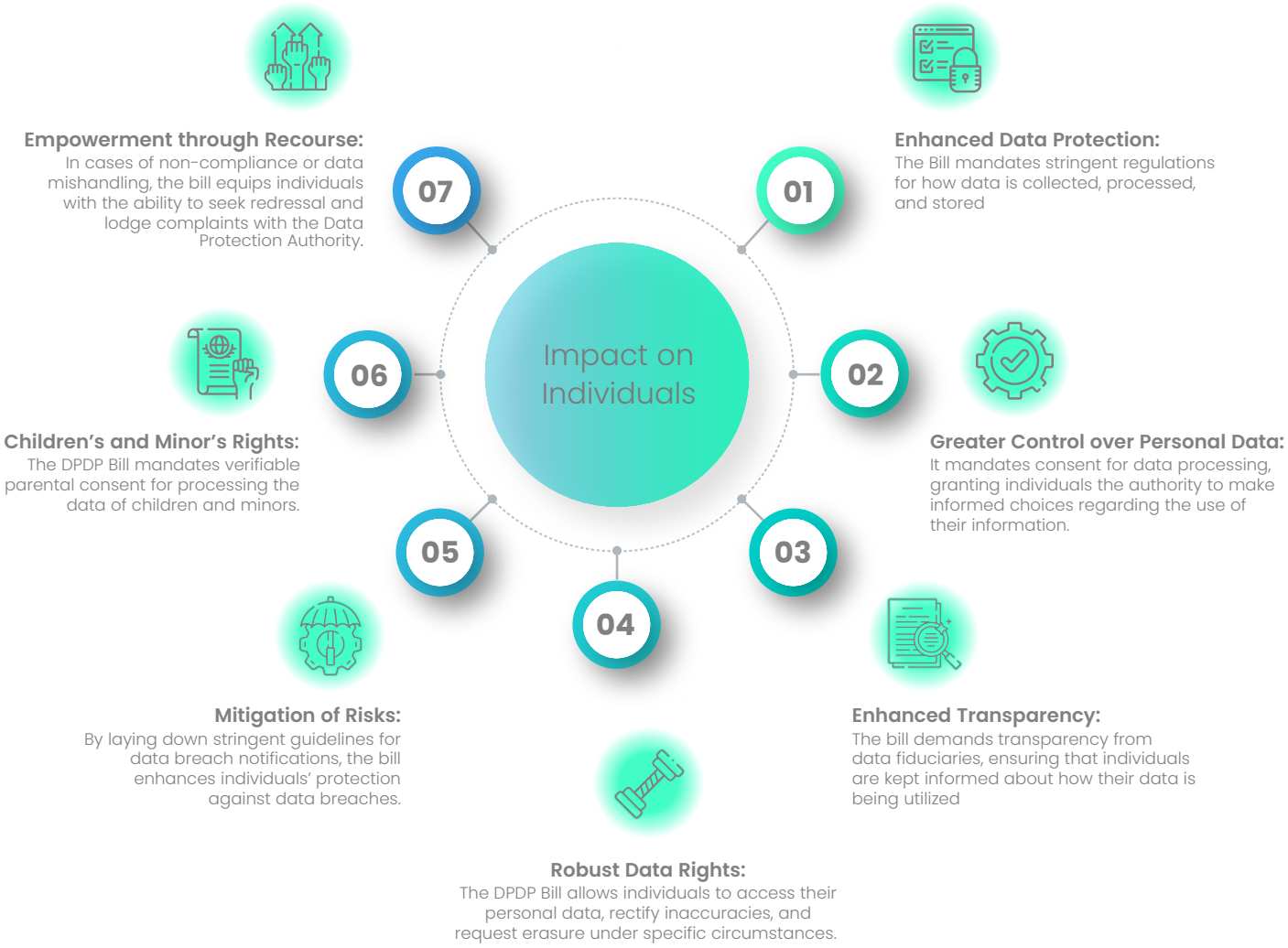
6

Miscellaneous Non-Compliance with the Bill's Provisions:
A penalty of up to INR 50 crore may be imposed for various forms of non-compliance with provisions stipulated in the Bill.

Chapter 4: Impact on Individuals and Businesses

The Data Protection Bill is poised to exert profound influences on both individuals and businesses. From affording greater control to personal data to enforcing data governance, we explore the various ways in which the Bill impacts both individuals and businesses in this chapter.

Impact on Individuals



Impact on Businesses

The DPDP Bill bears a substantial impact on businesses, prompting significant shifts in their operations and strategies as they navigate the intricacies of data protection and privacy in the digital realm. We've listed how it impacts businesses below.

Compliance and Legal Obligations: The bill ushers in a paradigm of compliance and legal commitments for entities handling data. Businesses and organizations find themselves obliged to meticulously follow these obligations. This encompasses obtaining explicit consent for data processing, ensuring data accuracy, instituting stringent security measures, and establishing frameworks for promptly notifying data breaches. The stakes of non-compliance are significant, ranging from financial penalties to potential harm to reputation.

Data Governance and Accountability: A robust culture of data governance and accountability becomes an indispensable requirement under the bill. To meet its standards, organizations need to formulate comprehensive policies and protocols for data handling. Aspects such as data minimization, purpose limitation, and storage constraints must be effectively addressed. The appointment of Data Protection Officers adds another layer of responsibility, compelling organizations to display accountability throughout their data processing operations.

Consent Management: Securing valid consent from individuals for their personal data processing is non-negotiable as per the bill. Businesses and organizations are necessitated to critically assess and possibly overhaul their consent management methodologies to align with the bill's stringent prerequisites. It further mandates transparent and lucid communication of processing intentions and extents to individuals, fostering an environment of informed data sharing.

Data Localization and Cross-Border Transfers: A notable aspect of the bill is its stance on data localization, mandating the storage of specific categories of personal data within the confines of India. This dictum carries potential implications for businesses with international operations or reliance on cross-border data transfers. Organizations must embark on comprehensive evaluations of their data storage and transfer modalities to ensure full alignment with the bill's tenets.

Impact on Business Models and Innovation: The bill's sweeping provisions could necessitate a reimagining of prevailing business models and data processing methodologies. Aspects of data-driven innovation might encounter substantial shifts due to heightened regulations and demands. Organizations are bound to grapple with added intricacies and constraints in their data utilization endeavors, prompting an introspection into operations and strategies to foster adaptability.

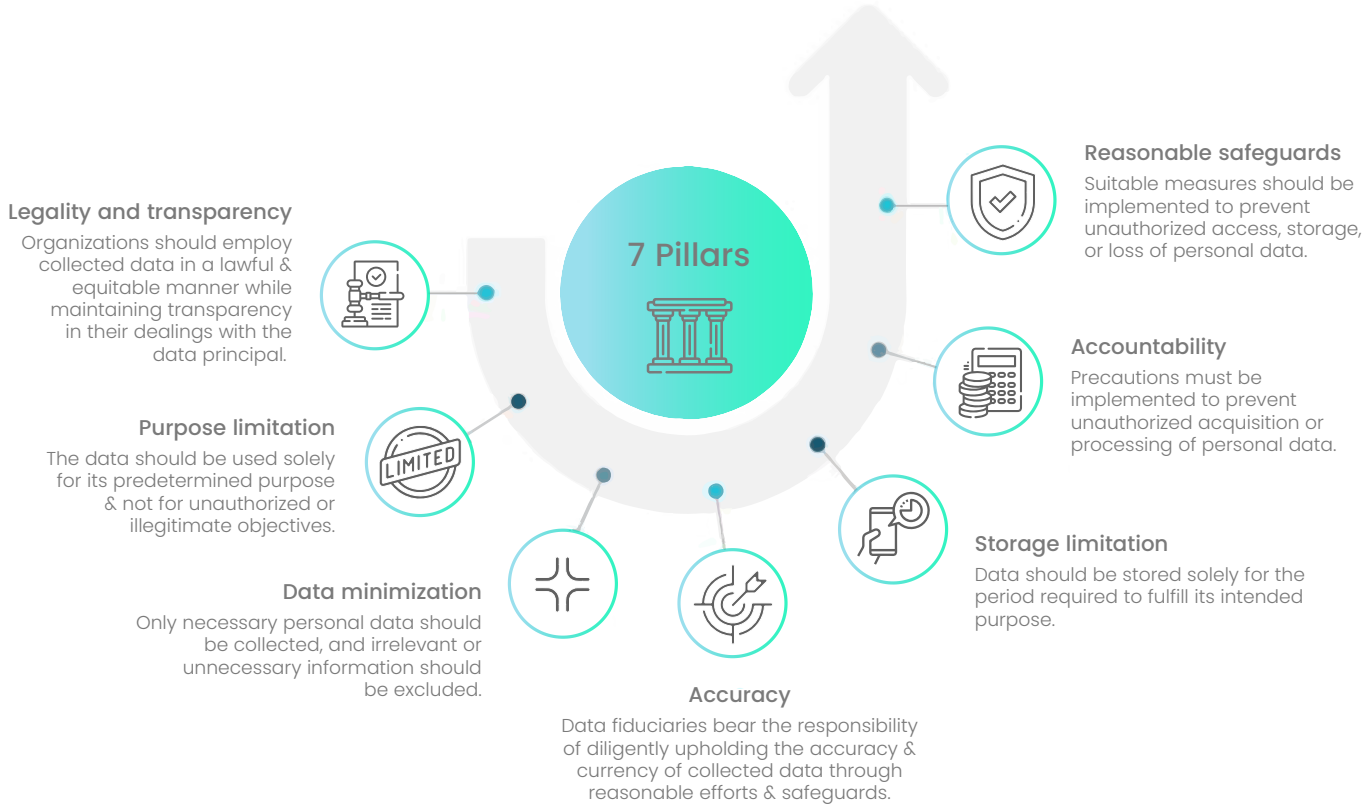
Increased Emphasis on Data Security: The bill underscores the criticality of robust data security and protection. Organizations must equip themselves with fitting technical and organizational measures to avert unauthorized access, breaches, and data misuse. The investment in fortified cybersecurity infrastructure and regular audits of security protocols becomes pivotal to upholding data integrity and safeguarding against potential vulnerabilities.

Chapter 5: Navigating the DPDP Bill

Navigating the DPDP Bill demands a strategic approach from businesses, encompassing both proactive measures and ongoing vigilance. By adopting a comprehensive and adaptive approach, businesses can effectively navigate the DPDP Bill, ensuring compliance, fostering trust, and contributing to a responsible and secure data ecosystem. We explore the best practices to navigate the Bill in this chapter.

Before we jump into the strategies, let's take a look at the seven core principles of the Bill, which provide a good understanding of what is required to navigate it.

Seven Core Pillars of the Bill



Strategies for navigating the DPDP Bill

By adopting the following strategic approaches, businesses can proactively navigate the complexities of the DPDP Bill, ensuring legal compliance, safeguarding data, and upholding ethical data handling practices in the digital age.

- **Hold Assessments and Audits:** Conduct a thorough assessment of existing data processing practices, identifying areas that require alignment with the bill's mandates. Perform data audits to gauge the scope, nature, and volume of personal data processed and identify potential risks.

- **Follow Privacy-by-Design:** Integrate privacy-by-design principles into product and service development processes. Consider data protection measures from the inception of new projects to embed compliance into the organization's DNA.

- **Conduct a Comprehensive Data Inventory:** Begin by conducting a thorough review of all the personal data that your organization collects, processes, and stores. Identify what kinds of data you deal with, why you process it, and the legal basis that allows you to do so.

- **Review and Update Policies:** Examine your current privacy policies, consent procedures, and how you handle data. Make necessary updates to make sure they align with the requirements of the data protection bill. This includes things like getting clear consent, collecting only necessary data, and respecting the rights of data subjects.

- **Establish Strong Data Management:** Set up a robust system for managing data within your organization. This involves defining who is responsible for data protection, appointing a Data Protection Officer if needed, and creating internal rules and procedures to follow the bill's rules.

- **Get Proper Consent:** Ensure that your procedures for getting consent follow the bill's rules. Make sure you're getting valid and clear consent from people. Explain what you'll do with their data and let them easily withdraw their consent if they want.

- **Boost Data Security:** Strengthen your security measures to keep personal data safe from unauthorized access and breaches. This could mean using encryption, controlling who can access the data, checking for vulnerabilities, and teaching your employees how to handle data safely.

- **Create a Plan for Data Breaches:** Prepare a plan for what to do if there's a data breach. This plan should include how to quickly identify and assess breaches, how to tell the people affected, and what actions you'll take to fix the problem and prevent it from happening again.

- **Train Your Employees:** Teach your employees about the data protection bill and how it affects their work. Give them regular training on the principles of data protection, best practices for privacy, and how your organization handles data.

- **Manage Relationships with Third Parties:** Look at your contracts with other companies that handle data for you. Make sure they follow the data protection bill's rules. Set up a good system for dealing with these companies, including checking how they protect data and making sure they follow the law.

- **Handle Data Subject Requests:** Create a process for handling requests from people about their data. This could be requests to access, correct, delete, or object to their data. Make sure this process is clear, fast, and follows the bill's rules.

- **Stay Informed and Get Legal Advice:** Keep up-to-date with any news or guidance from the Data Protection Board and other authorities. They'll help you understand how to follow the data protection bill. If you need help with specific questions, consider getting advice from legal experts who know about data protection laws.

Conclusion

The Digital Personal Data Protection Bill stands as a significant milestone in India's journey towards safeguarding individual privacy and data protection in the digital age. This comprehensive legislation brings to the forefront a multitude of principles, mandates, and mechanisms aimed at reshaping the landscape of data handling, processing, and storage.

From the establishment of a vigilant Data Protection Board to the redefinition of consent management and the fortification of data security measures, the bill encapsulates a holistic framework that champions the rights of data principals while setting the standards for responsible data handling.

The DPDP Bill provides a roadmap for businesses to navigate the complexities of data protection and privacy. By embracing transparency, accountability, and ethical data practices, organizations can not only adhere to the bill's stipulations but also cultivate trust and goodwill among stakeholders.

Nevertheless, this endeavor presents its own challenges. Balancing new obligations alongside operational and business goals can be demanding for organizations.

This is where Scrut comes in. We have extensive experience in helping companies navigate diverse compliance frameworks. We acknowledge the complexities of regulatory adherence and strive to make the process as smooth as possible for you. Whether it entails implementing security controls or managing vendor relationships, we will accompany you every step of the way. If you seek the expertise of seasoned professionals to navigate this new framework, feel free to connect with us!

For individuals, the bill reinforces the fundamental right to privacy, placing control over personal data firmly in their hands. As technology continues to evolve, the DPDP Bill assures that the digital footprint we leave behind is shielded from unwarranted intrusion and exploitation.

It is imperative to recognize that the journey towards comprehensive data protection is not a destination but an ongoing endeavor. The DPDP Bill sets the stage for a dynamic interplay between technology, law, and society. It challenges us to adapt, innovate, and uphold the principles of privacy and data protection in a digital landscape that is ever-changing.

As India strides forward into this new era of data governance, the DPDP Bill offers a clarion call for collaboration, awareness, and responsible action. By working together, individuals, businesses, and policymakers can forge a future where technology thrives in harmony with privacy, ensuring that the digital realm remains a sanctuary of rights, opportunities, and progress for all.