SOUTH INDIAN Bank
EXPERIENCE NEXT-GEN BANKING

Students' ECONOMIC FORUM

A monthly publication from South Indian Bank

To kindle interest in economic affairs...
To empower the student community...

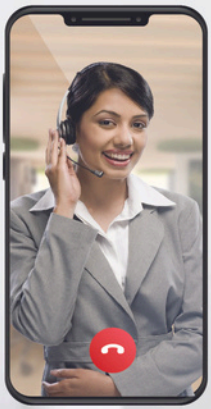
www.southindianbank.com
Students' Corner
ho2099@sib.co.in

The DPDP Act, 2023

November 2025 | Theme 407

SOUTH INDIAN Bank
EXPERIENCE NEXT-GEN BANKING

OPEN AN ACCOUNT
ANYTIME, ANYWHERE
IN JUST A FEW MINUTES!

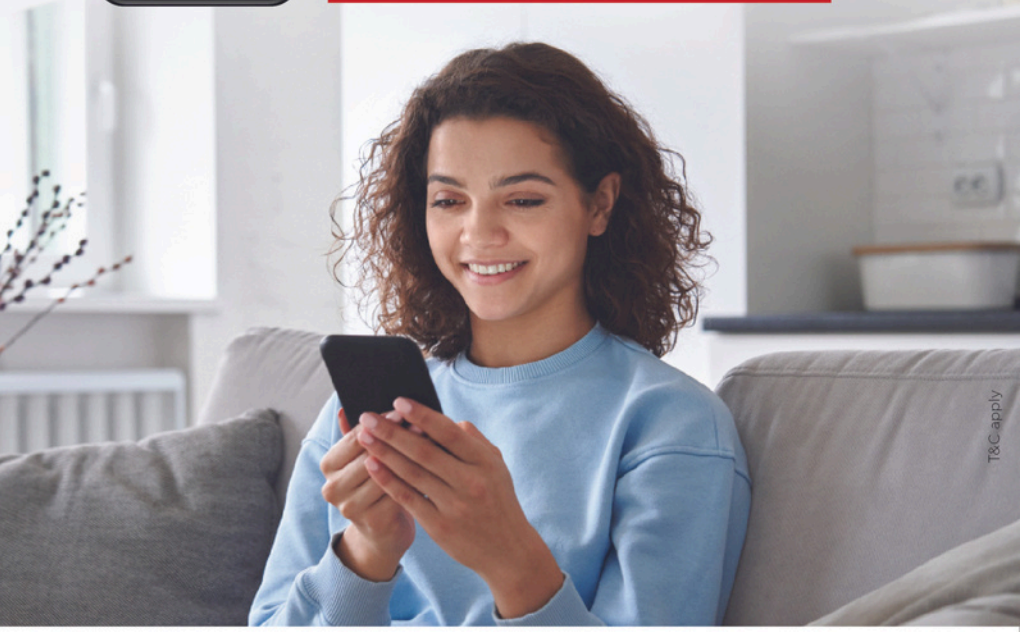


Scan to Apply

With Video KYC Account Opening

Banking simplified!

Aadhaar Card + PAN Card + Video Call to open your Savings Account.



T&C apply

"Data protection is not just about security; it is about the dignity of the individual in the digital age."
Narendra Modi, Prime Minister of India

Nov 2025 | Theme 407

The 'SIB Students' Economic Forum' is designed to kindle interest in the minds of the younger generation. We highlight one theme in every monthly publication. Topics of discussion for this month is **The DPDP Act.**

For the better part of two decades, the Indian digital economy operated in a regulatory environment often compared to the "Wild West."

Data - the digital footprint of a billion citizens - was extracted, refined, and monetized with minimal oversight.

While the Information Technology Act of 2000 provided a basic framework, it was ill-equipped to handle the complexities of AI, Big Data, and algorithmic processing.

On August 11, 2023, this era formally concluded. With the Presidential assent to the **Digital Personal Data Protection (DPDP) Act, 2023, India** established a modern, robust framework that redefines the relationship between the citizen and the corporation.

For students of economics, commerce, and law, the DPDP Act is not merely a compliance checklist; it is a structural reform. It transforms "Personal Data" from a free commodity into a regulated asset class, altering the cost of doing business and the value of consumer trust.

This edition of SEF provides a comprehensive analysis of the Act's architecture, its economic implications, and the new rights it bestows upon the Indian citizen.

1. The Philosophical Shift: *From Control to Trust*

To understand the letter of the law, one must understand its spirit. Unlike the European Union's GDPR, which is often viewed as a rights-centric model focusing heavily on privacy as a fundamental human right, the Indian DPDP Act attempts a unique balancing act. It seeks to

harmonize the individual's right to protect their personal data with the necessity of processing that data for lawful purposes - be it business innovation or state welfare.

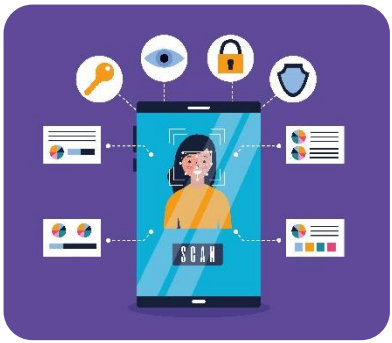
The terminology reflects this shift. The Act abandons the adversarial terms "Data Controller" and "Data Subject." Instead, it introduces:

Data Principal: The individual to whom the data belongs.
Data Fiduciary: The entity processing the data. The word "Fiduciary" is significant; in law, a fiduciary relationship is one based on trust (like a doctor-patient or banker-client relationship).

By using this term, the Act implies that companies are merely custodians of data, not owners, and they owe a duty of care to the individual.

2. Scope, Jurisdiction, and exemptions

The Act is precise in its application. It covers *"digital personal data,"* defined as data collected in digital form or non-digital data that is subsequently digitized.



This implies that a purely paper-based record system that is never scanned or typed into a computer falls outside the Act's purview - a nudge towards digital modernization, ironically.

The Long Arm of the Law: Crucially, the Act possesses extra-territorial jurisdiction. It applies to the processing of personal data outside India if such processing is in connection with offering goods or services to Data Principals within India. This ensures that global tech giants cannot evade Indian law simply by locating their servers in Ireland or Singapore. If they target Indian consumers, they must play by Indian rules.

The "Start-Up" Exemption: Recognizing that compliance costs can stifle innovation, the Act empowers the Central Government to exempt certain classes of Data Fiduciaries, including startups, from specific provisions like the Right to Access or the Notice requirement. This is a deliberate policy choice to ensure the Indian startup ecosystem remains agile.

3. The Architecture of Consent

At the heart of the DPDP Act lies the principle of Consent *(Section 6)*. However, the Act raises the bar for what constitutes valid consent. It must be **"free, specific, informed, unconditional, and unambiguous,"** provided through a clear affirmative action.

This effectively bans the "dark patterns" often used by apps - such

as pre-ticked checkboxes, confusing double-negatives in privacy policies, or making "Yes" buttons bright green and "No" buttons invisible grey.

The Notice Requirement: Before seeking consent, a Fiduciary must present a Notice *(Section 5)*. This Notice serves as a transparency tool. It must clearly state:

1. The personal data to be collected.
2. The specific purpose of processing.
3. The way the user can exercise their rights or file a complaint. To ensure true inclusivity, the Act mandates that this Notice must be available in English and all **22 languages** specified in the Eighth Schedule of the Constitution. This ensures that a Tamil speaker in rural Madurai has the same level of informed consent as an English speaker in Mumbai.

4. "Certain Legitimate Uses": The Pragmatic Approach

The drafters of the Act recognized that demanding explicit consent for every minor interaction would lead to "consent fatigue," where users mindlessly click "Agree" just to get it over with.

To solve this, Section 7 introduces **"Certain Legitimate Uses"** (previously discussed as "Deemed Consent").

This section allows processing without explicit consent in logical scenarios:

- **Voluntary Action:** If you give your phone number to a restaurant to get a waiting list update, you have voluntarily provided data for a specific purpose. The restaurant doesn't need to show you a legal notice for that.
- **Employment:** Employers can process employee data for payroll, benefits, or protecting trade secrets without needing fresh consent for every action.
- **State Functions:** The State can process data to provide subsidies, benefits, certificates, or licenses.
- **Public Order:** Data can be processed to fulfil legal obligations or comply with court judgments.

5. The Rights of the Data Principal

The Act empowers the Indian citizen with a suite of digital rights, creating a mechanism for accountability.

Right to Access (Section 11): A Data Principal can ask a Fiduciary for a summary of their personal data and the identities of all other Data Fiduciaries and Data Processors with whom the data has been shared. This brings transparency to the "data supply chain."

Right to Correction and Erasure (Section 12): This is often called the "Right to be Forgotten." A user can demand the correction of inaccurate data. More importantly, they can

demand the erasure of their data once the purpose for which it was collected is served.

For example, if you close an e-commerce account, you can demand they delete your address and purchase history, unless they are required by tax laws to keep it for a specific period.

Right to Grievance Redressal (Section 13): The Act mandates that every Fiduciary must have a grievance redressal mechanism. A user cannot be made to run from pillar to post; there must be a clear channel to file complaints, and the Fiduciary is legally obligated to respond.

Right to Nominate (Section 14): This is a pioneering feature in global privacy law. A Data Principal has the right to nominate another individual who shall exercise their rights in the event of their death or incapacity.

This effectively creates a legal framework for "Digital Inheritance," acknowledging that our digital lives (emails, photos, assets) survive us.

6. Obligations of the Significant Data Fiduciary (SDF)

The Act operates on a tiered compliance model. While all Fiduciaries have basic obligations (security safeguards, breach notifications), the government will designate certain entities as Significant Data Fiduciaries (SDFs) based on the volume and sensitivity of data they handle. Banks, telecom operators, health tech companies, and large social media platforms will fall into this category.

SDFs face a much stricter compliance regime:

1. **Data Protection Officer (DPO):** They must appoint a DPO based in India who serves as the point of contact for the grievance redressal mechanism.

2. **Independent Data Auditor:** They must appoint an independent auditor to conduct periodic audits of their compliance.

3. **Periodic Data Protection Impact Assessment (DPIA):** Before launching new technologies or processing strategies, they must conduct a formal assessment of the risks to the rights of Data Principals.

7. Protecting the Vulnerable: Children and Persons with Disabilities

The Act places a "protective ring" around children (defined as those under 18).

- **Verifiable Parental Consent:** Fiduciaries must obtain verifiable consent from a parent or lawful guardian before processing a child's data.

- **The "No-Go" Zones:** Fiduciaries are strictly prohibited from tracking, behavioural monitoring, or directing targeted advertising at children. They also cannot process data in any way that is likely to cause a "detrimental effect" on a child's well-being.

- **Note on Education:** The government retains the power to exempt certain educational or health platforms from the strict parental consent rule to ensure that access to essential services is not hindered.

8. The Enforcement Mechanism:

The Data Protection Board of India
The Act establishes the Data Protection Board of India (DPBI).

Unlike sector-specific regulators (like RBI or SEBI) that issue licenses and regulations, the DPBI is designed primarily as an adjudicatory body. It acts as a specialized court for data issues.

Role: Its main functions are to inquire into data breaches, investigate complaints (after the user has exhausted the Fiduciary's grievance mechanism), and impose penalties.

Digital by Design: In a bid to avoid the notorious delays of the Indian legal system, the Act mandates that the Board's proceedings be digital "as far as practicable," aiming for swift resolution of disputes.

Appeals: Any person aggrieved by an order of the Board can appeal to the Telecom Disputes Settlement and Appellate Tribunal (TDSAT), and subsequently to the Supreme Court of India.

9. The Penalty Regime:

Deterrence over Criminalization

The DPDP Act marks a shift in Indian jurisprudence by decriminalizing privacy violations. There are no jail terms for company executives. Instead, the Act relies on massive financial penalties to ensure compliance. The penalties are capped based on the nature of the violation:

Violation	*Maximum Penalty*
Failure to take reasonable security safeguards to prevent a data breach	₹250 Crore
Failure to notify the Board or affected users of a breach	₹200 Crore
Breach of obligations regarding Children's Data	₹200 Crore
Breach of obligations by Significant Data Fiduciaries	₹150 Crore
Breach of duties by the Data Principal (User)	₹10,000

Crucially, these penalties apply per instance. This means a repeated or continuous violation could theoretically lead to cumulative fines far exceeding the caps for a single instance.

10. Cross-Border Data Flows: The "Negative List" Approach

For years, the debate on "Data Localization" (forcing companies to store data only in India) stalled the legislation. The 2023 Act resolves this with a pro-business compromise. It allows the transfer of personal data to any country or territory outside India, except those specifically restricted by the Central Government.

This "Negative List" approach is a boon for the IT and BPO sectors. It allows Indian companies to seamlessly serve global clients and allows multinational corporations to process Indian data in global hubs, provided those hubs are not in hostile or blacklisted jurisdictions. However, sector-specific restrictions (like the RBI's mandate on payment data storage) continue to apply and override the general permissions of the DPDP Act.

The enactment of the DPDP Act is only the beginning. The "rules of the game" will be fully defined when the subordinate legislation (the Rules) is notified. These rules will clarify the specifics: How does one verify parental consent? What exactly constitutes a "significant" fiduciary? What is the format of a data breach notice?

For the Indian economy, the Act represents a maturation. It aligns India with global standards like the GDPR, making it a more attractive destination for foreign investment. For the student and the citizen, it offers a promise: that in the vast, invisible flow of digital information, they remain the ultimate sovereign of their own data. The era of "Data as the new Oil" continues, but now, the oil wells are guarded.

References:

1. *The Digital Personal Data Protection Act, 2023 (No. 22 of 2023).*
2. *Notification of the Digital Personal Data Protection Rules, 2025*
3. *The Digital Personal Data Protection Bill, 2023: Bill Summary & Analysis. Institute for Policy Research Studies, New Delhi.*

SIB Mirror+

SOUTH INDIAN Bank
EXPERIENCE NEXT-GEN BANKING

THE BANK ON YOUR PHONE, SIB MIRROR+

- Available in 9 different languages
- Instant payment to 100+ billers
- Secure your account with e-Lock feature

Scan & download the SIB Mirror+ App Now!

T&C apply

SIB Car Loan

SOUTH INDIAN Bank
EXPERIENCE NEXT-GEN BANKING

UP TO 100% FINANCE

ON YOUR CAR'S ON-ROAD PRICE

Scan to Apply

T&C apply

DRIVE YOUR DREAM CAR WITH SIB CAR LOAN

Tenure
up to 7 years

Loan for new and
used cars

Easy
documentation

SOUTH INDIAN Bank
EXPERIENCE NEXT-GEN BANKING

Introducing

Her account

Banking, Redefined for Women

- Milestone Rewards
- Exclusive Her Debit Card
- Exclusive Insurance Benefits

Open your HER Account today

*T&C Apply.


SOUTH
INDIAN Bank
EXPERIENCE NEXT-GEN BANKING