DPDPA Compliance & Indian Banks

How wide is the gap between ‘As-is’ and ‘Should-be’

Welcome to **the Age of Data Privacy**

Ashok Hariharan, CEO IDfy

The DPDP Act is not a mere checkbox for organizations; it represents a paradigm shift in the way companies approach the full user lifecycle. It necessitates a thoughtful consideration of each specific purpose for which data is collected.

The DPDP Act demands a meticulous approach to the user data lifecycle. Data fiduciaries must not only secure consent but also regularly manage instances of consent updates or withdrawals.

They must also extend this responsibility to ensure that all outsourced partners, or data processors, handle user data responsibly. Compliance with the DPDP Act also requires a cultural transformation for organizations. By embedding data privacy into the organizational culture, companies can use compliance as a tool to build and maintain user trust.

The DPDP Act, 2023, heralds a new era in data protection, urging organizations to rethink their approach to user data. The enactment of the DPDP Act is an invitation for organizations to embark on a transformative journey towards a privacy-centric future.

Research Methodology

Investigating Data Privacy in Banking Journey

STEP 1 | **Product Journey Analysis**

We analysed 25[1] digital journeys of the top 10 banks in India, across 4 use cases:

1. Savings Bank Account
2. Personal Loan
3. Education Loan
4. Home Loan

The analysis was divided into 4 phases:

1. Personal Data collection analysis
2. Privacy Documents review
3. Terms & Conditions review
4. Dark Pattern identification

Note 1: While there were 40 journeys, only 25 were digital, hence, the rest have not been analyzed.

1. Personal Data

Data fields within banking journeys were listed, and PII data fields were categorized as sensitive or non-sensitive.

PII Data

Information about an individual, including Personally Identifiable Information (PII), which, alone or in combination with other data, can identify a person

Sensitive Data

Piece of PII data that can independently identify an individual without the need for additional identifiers. Eg. Account number, PAN number, Aadhaar number

Non Sensitive Data

Identifiers that need one or more such data points to identify an individual. Eg: gender, age, first name, date of birth

2. Privacy Documents

Privacy documents were scrutinized for DPDP 2023 compliance, identifying various non-compliance issues grouped into 6 categories namely presence of Aggregated purposes, Consents with unspecific duration, consents that are unclear and vague, consents regarding unsolicited data sharing, consents regarding cross-selling and non-presence of grievance officer contact details.

3. Terms and Conditions (T&C)

Terms and Conditions of different banks were examined, revealing numerous non-compliant consents.

4. Dark Patterns

Privacy Documents and T&C were analyzed to identify dark patterns, including vague purposes, unsolicited data sharing, misleading consent durations, and lack of clear purposes.

STEP 2 **Bank Cookie Analysis**

There are 5 types of cookies that we doubled down on; here's what each cookie is used for:

Necessary Cookies

Essential for website functionality, enabling user navigation and secure access.

Example: User authentication and session management.

Performance Cookies

Optimize website efficiency by monitoring and improving performance.

Example: Tracking website traffic, and resolving performance issues.

Functional Cookies

Enhance user experience by providing personalized features and settings.

Example: Remembering preferences like language settings or customizations.

Advertising Cookies

Collect data for targeted advertising and measuring ad effectiveness.

Example: Displaying personalized ads based on user interests and behavior.

Analytics Cookies

Collect aggregated, anonymous data on website usage to understand user interactions and optimize performance.

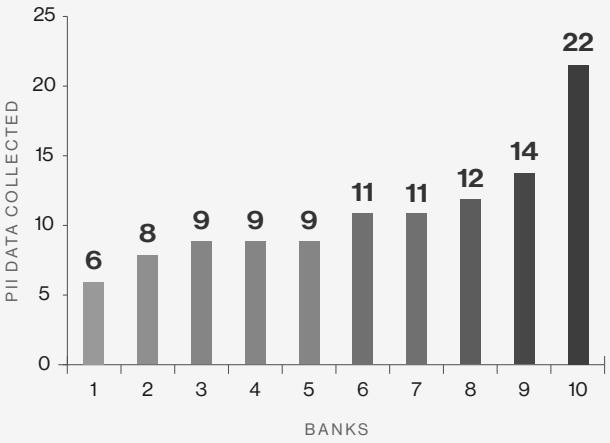
Example: Tracking page views, popular content, and user interactions.

How much data do we really need?

Embracing Data Minimization not only enhances the safety and security of user data by collecting only essential Personally Identifiable Information (PII) but also mitigates risks of unauthorized access, fostering responsible data stewardship. However, there appears to be a lack of consensus among banks regarding the amount of PII data necessary for customer verification and onboarding, as evidenced by variations in data collection practices for the same product.

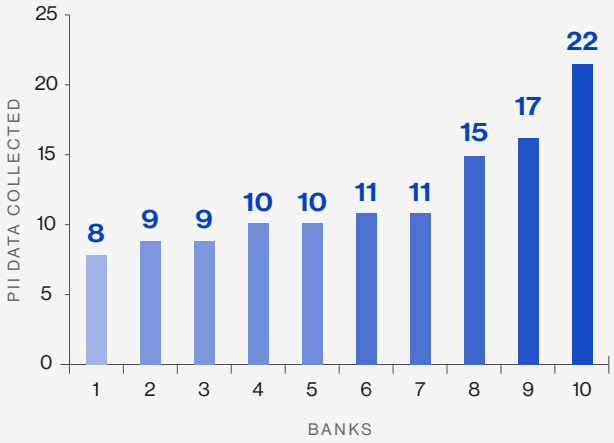
Look at the stark contrast between the data points collected, for these 2 use cases:

Savings Account journey



Bank 1 can complete the onboarding with 6 PII data points whereas Bank 10 collects 22 PII data points for the same use case.

Personal Loan journey



Bank 1 can complete the onboarding with 8 PII data points whereas Bank 10 collects 22 PII data points.

9/10 banks did not mention the PII data collected in their privacy policy.

How much is too much?

The quest for personal information often treads a fine line between “must have” and “good to have”. Here are the PII data fields that the banks need to closely examine and ask themselves if they really need it.

Savings Account

PII	No. of Banks
Occupation	6
Employer’s name	6
Employment type	4
Professional email	3
Years of Experience	2
Past Employer	1
Education	1
College Name	1
Marital status	4
Religion	1
Caste	1
Spouse’s name	1
Father’s name	4
Mother’s name	4

Personal Loan

PII	No. of Banks
Employer’s name	4
Work Experience	4
Designation	4
Past Employer	2
Years of Experience	2
Professional email ID	4
Education Qualification	2
Caste	1
Father’s name	5
Mother’s name	2
Spouse’s name	2
Marital status	2

1. Details pertaining to professional background

An individual’s professional background can vary in necessity. While certain details such as years of experience are typically “must-have” for assessing financial stability and capability, others like the name of one’s college or past employers could be omitted unless there is a pressing need for it.

2. Marital status, religion, caste

These categories are particularly sensitive and often irrelevant to the core function of banking services. While collecting marital status for joint accounts might seem legitimate, religion and caste seem completely irrelevant in almost all banking services. Banks must exercise caution in soliciting such information to avoid discriminatory practices and breaches of privacy.

3. Spouse name, father’s name, mother’s name

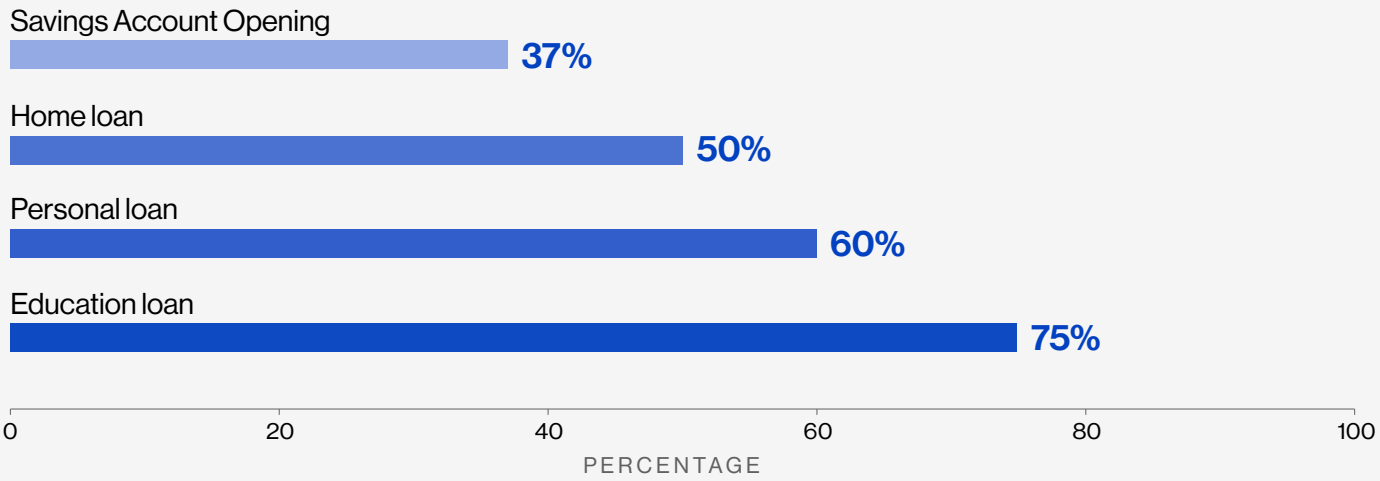
These details in banking applications warrant scrutiny due to various intended purposes. These may include cross-selling products to family members or obtaining parental consent when the data principal is below 18 years old.

How sensitive are we about data?

A high percentage of ‘sensitive PII data’ is being collected across the Banks we studied. This is true for almost all journeys. Data is considered sensitive when it can be used to uniquely identify an individual.

Examples of sensitive data include PAN & bank account number. There is, however, a significant difference in the PII collected between different journeys. Education loans typically ask for a higher percentage of sensitive data.

Average percentage of PII data collected that is sensitive



Did you know?

Of all the PII Data collected by a bank for an educational loan process, 84% was found to be sensitive PII Data

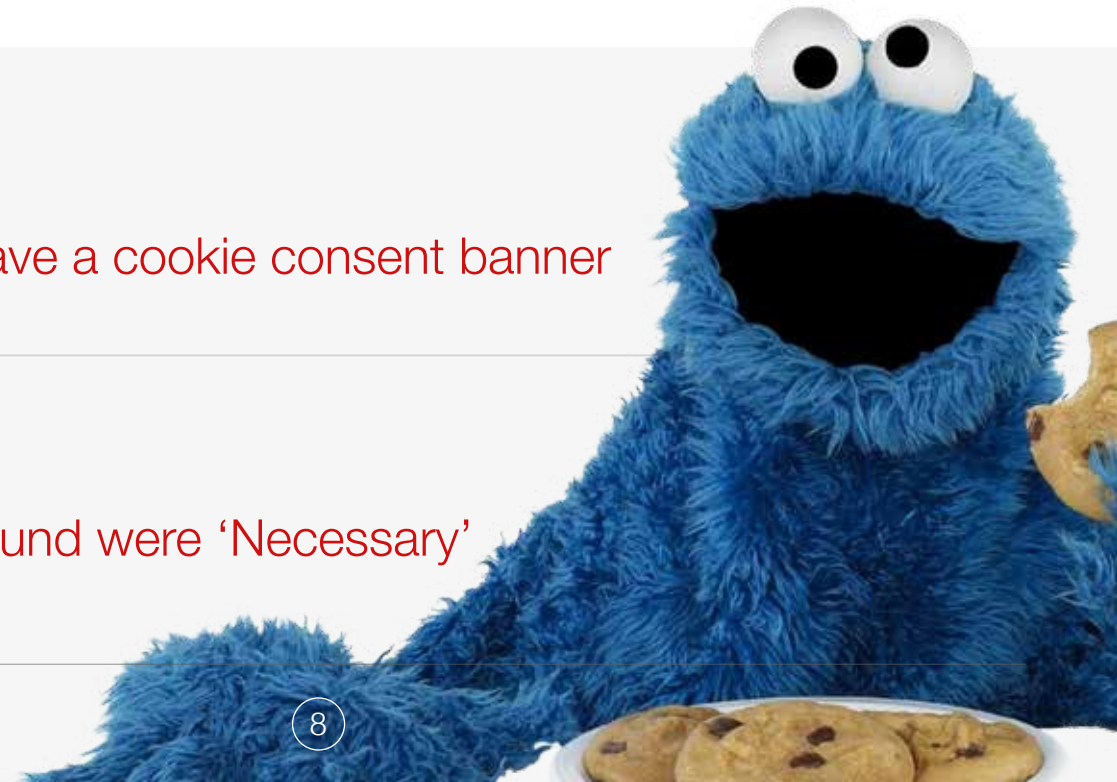
The Cookie crumbles on Consent

The globally accepted policy for website cookies involves obtaining user consent, utilizing essential cookies, and being transparent about the use of cookies for advertisements and cross-selling.

Some cookies can lead to de-anonymizing users. This can lead to compromising the user's PII data. This is where consent becomes especially critical.

Here's how Indian Banks are doing on their website cookies

- 10/37 cookies found on one bank's website were unknown/malicious
- 70% of all cookies found on a leading bank's website were for Marketing & Analytics
- One of the Banks had a total of 103 Cookies on their website
- 2/10 banks did not have a single Necessary cookie on their website
- Nearly 25% of all cookies found on a Bank's website were categorized as Unknown.



9/10

Banks did not have a cookie consent banner

Only 7%

of the cookies found were 'Necessary'

Consent Commandments

Expectation vs Reality

Thou shalt take explicit consent

0/10 Banks are taking explicit consent

Thou shalt make grievance handling accessible

4/10 Do not have Grievance Officer contacts mentioned in Privacy Policy

---

Thou shalt make consent notice unambiguous

9/10 Banks had misleading or unclear policies (and zero did it in 22 languages)

Thou shalt mention all personal data being collected mapped with their purposes

1/10 Banks mentioned personal data being collected in their privacy policies

---

Thou shalt take parent's consent for processing of child's data

0/10 Banks collected parent's consent

Thou shalt take principal's consent for cookies on the website

1/10 Banks collected cookie consent

Thou shalt take explicit consent for marketing and cross selling

0/10 Banks asked for an explicit consent

Thou shalt not take blanket consent

0/10 Banks took specific permissions for different purposes

Thou shalt mention specific purpose when taking consent to share data with other parties

5/10 Banks did not mention the purpose while taking consent to share data with other parties

Thou shalt have separate consent notices for each customer journey

10/10 Banks took consolidated consent that had multiple purposes

What are Dark Patterns in Privacy Policy documents?

They are policy documents that have vague purposes, unsolicited data sharing, misleading consent durations, a lack of clear purposes, and blanket consent for unspecified purposes among others.

Did you know of the dark patterns that could exist in your current consent journey?

☑ I seek from the Bank various financial assistance, other products and services for which I may be found eligible by the Bank from time to time, at any time in future, including after closure of any of my existing or future relationships, accounts, products, facilities, loans, services with or from the Bank from time to time, for which purpose I authorize the Bank to share any of my Information (as defined hereinafter) with any credit information companies and obtain various scores, reports and information for determining my credit worthiness from them, and accordingly to contact me or cross sell to me from time to time.

- Aggregated purposes
- Consent duration vague and not specific
- Ambiguous language
- Taking lifetime consent to cross-sell

About PRIVY

PRIVY by **IDfy** is India's only Consent Governance solution for digital data protection and privacy as per provisions of the DPDP Act.

PRIVY provides a platform for enterprises to manage user consent regarding Personally Identifiable Information (PII) data, ensuring that data is handled precisely as per the user's consent. As a part of its solution, PRIVY includes InspectAI, an AI-driven tool for Gap analysis.

Inspect AI uses AI models to review an organization's current processes and practices around user data. It provides a detailed and actionable analysis of the gap to be bridged for DPDP compliance.

PRIVY, as a full-stack consent governance solution, delivers two critical functions.

1

User Empowerment

PRIVY simplifies user consent, allowing easy review, approval, and adjustments to data permissions.

2

Consent Compliance

The platform guides enterprises to ensure that user data is utilized in strict adherence to the consent provided. This not only fosters customer trust but also ensures compliance with the DPDP Act.

PRIVY provides analytics dashboards for the organization's Data Protection Officer (DPO) to have a real time enterprise-wide view of data usage and consent.

Eliminate Fraud.
Establish Trust.

IDfy is an Integrated Identity Platform offering products and solutions for KYC, KYB, Background Verifications, Risk Assessment, and Digital Onboarding.

We establish trust while delivering a frictionless experience for you, your employees, customers and partners.

Only IDfy combines enterprise-grade technology with business understanding and has the widest breadth of offerings in the industry.

With more than 12+ years of experience and 2 million verifications per day, we are pioneers in this industry.

Our clients include HDFC, IDFC, IndusInd, Axis, RBL, Equitas, PhonePe, Amazon, and others.

shivani@idfy.com

www.idfy.com