



Finance Industry Development Council(FIDC)

Digital Personal Data Protection Act, 2023

November 2025
Private and confidential

Contents

- 1 Setting the Context
- 2 What is Personal Data in the NBFC Context ?
- 3 The Digital Personal Data Protection Act : What It Means for NBFCs
- 5 An Overview of Privacy Tools
- 4 Questions

November 2025



Setting the Context



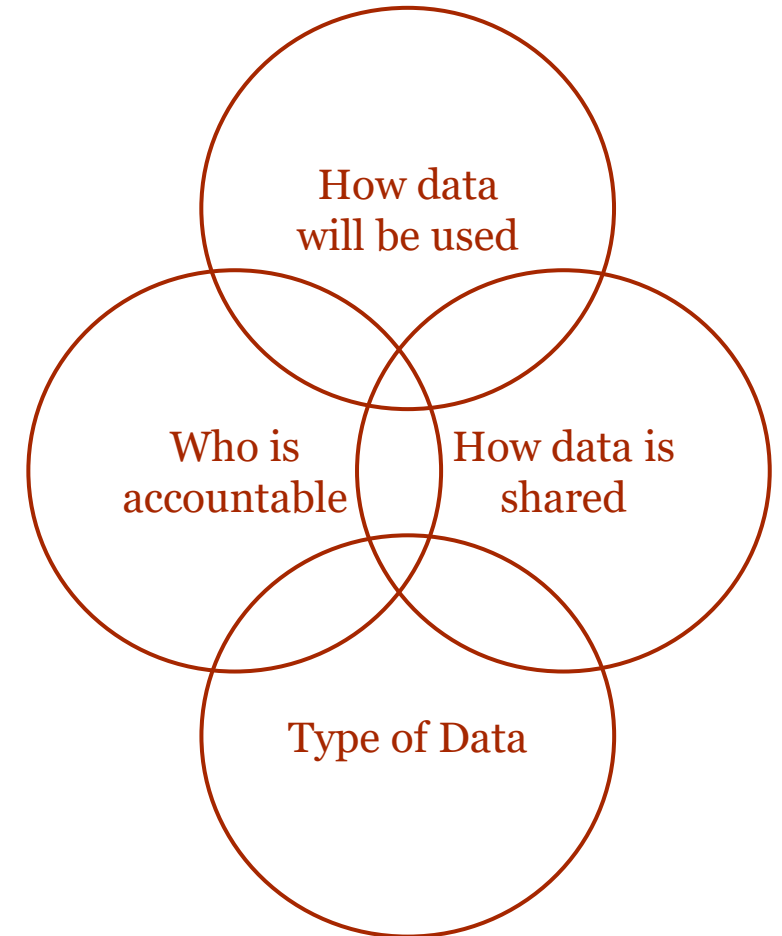
November 2025

What is Data Privacy?

Privacy encompasses the **rights of individuals** and **obligations of organizations** with respect to the **collection, use, retention, disclosure, and disposal** (“processing”) of personal data (i.e., across the data life cycle).

Data privacy is focused on the use and governance of personal data. It is typically **associated with the proper handling of personal data.** The rights of an individual to control how their own personal data is **collected, used, and disclosed** to others.

Key Considerations



Need for Data Privacy and Protection

While data can be put to beneficial use, the **unregulated and arbitrary use of data, especially personal data**, has raised **concerns regarding the privacy and autonomy of an individual**.



WITHOUT DATA PRIVACY AND PROTECTION:



Increased Surveillance



Profiling of Individuals



Data and Identity Theft



An Impact on individual independence



Free flow of personal data in the digital age, multiple touchpoints of data collection and processing, and the above-mentioned threats have led to a need for a holistic approach to data privacy and protection.

What is Personal Data in the NBFC Context ?



November 2025

What is Digital Personal Data in the context of NBFC sector

Personal Data means any data about an individual who is identifiable by or in relation to such data.

Digital personal data means personal data in digital form.

General Personal Data

- Full name
- Gender
- Date of birth and age
- Marital status
- Citizenship and nationality
- Residential and business addresses
- Phone numbers (personal and business)
- Email addresses
- Government-issued IDs (e.g., PAN, Aadhaar, Voter ID)
- Internal customer IDs or account numbers

Customer Personal Data

- Income documents (salary slips, ITRs)
- Credit bureau reports (CIBIL, Experian, etc.)
- Loan account numbers
- Personal financial details (e.g., bank statements, ITRs)
- Credit scores and bureau reports
- Transaction history (EMIs, repayments, defaults)
- Income and asset declarations

Employee Personal Data

- Employment history
- Employee relations
- Compensation/remuneration related matters
- Payroll
- Background investigation reports
- Health and benefits data
- Employee relations and disciplinary records

Other Personal Data

- Photographs (from KYC or video KYC)
- Family details (e.g., co-applicants, nominees)
- Contact references
- Certificates and licenses (e.g., business registration for MSME loans)
- Demographic data (location, occupation)
- Biometric data (e.g., fingerprint or facial recognition for eKYC)
- IP addresses and device metadata (from digital platforms)
- CCTV footage

The above list is not exhaustive and is only for indicative purposes.

The Digital Personal Data Protection Act: What It Means for NBFCs



November 2025

Evolution of DPDP Act

Shikrishna Committee

The foundation for India's modern data protection framework was laid by the Justice B.N. Srikrishna Committee, formed in 2017. through its report - "A Free and Fair Digital Economy" released in 2018

2017-2018



Personal Data Protection (PDP) Bill

The first draft introduced in parliament included provisions of a Data Protection Authority (DPA) to oversee compliance and introduced individual rights

2019



2022

Withdrawal of PDP Bill

The government withdrew the PDP Bill, citing the need for a simpler, more focused framework.

Digital Personal Data Protection (DPDP) Act

The DPDP Act, became an Act in August 2023, provided for processing of digital personal data in a manner that recognizes both the right of individuals to protect their data and the need to process such personal data for lawful purposes. It also introduced the Data Protection Board as the regulator for DPDP

2023



2025

Draft Rules for DDPD Act

The draft DPDP Rules, released for public consultation in January 2025, provided clarity some of the tenets of the DPDP Act and aimed to provide guidelines for operationalization of the DPDP Act.



2025

Final Rules for DDPD Act

The Final DPDP Rules, released in November 2025, notified the implementation timelines of 18 months for key aspects of the Act and 12 Months for establishment of consent manager.

The DPDP Act 2023 & Final Rules 2025

The Act applies to

01

within the Indian territory



to the processing of digital personal data within the territory of India, where the personal data is collected in a:



01 a) digital form

01 b) personal data collected is in non-digital form and digitized subsequently.

02

outside the Indian territory



to processing of digital personal data outside the territory of India, if such processing is in connection with:

02 a) any activity related to offering of goods or services to data principals within the territory of India.

The Act doesn't apply to

- personal data processed by an individual for any personal or domestic purpose; and
- personal data that is made or caused to be made publicly available by the data principal to whom such personal data relates
- person who is under an obligation under any law for the time being in force in India to make such personal data publicly available.

Final Rules outline nuances of the Act:

1

Privacy Notice needs to be itemized, and purpose led. Consent withdrawal to be equally easy as providing consent

2

Reasonable security safeguards has been expanded significantly in the Rules

3

Breach reporting timelines to DPB and principals have been given as 72 hours

4

Some exemptions on state and its instrumentalities as well as on statistical and research etc. has been provided

5

Child data, PWD data identification as well data nominations have been elucidated

6

Rules now require Data Fiduciaries to retain personal data and logs for a minimum of one year post-processing



The Act and Rules provide for an onerous responsibility and implementation exercise for the companies.

The DPDP Act 2023 & Final Rules 2025

The Indian government has issued a set of 23 rules for the Digital Personal Data Protection (DPDP) 2025. These rules aim to enforce the Digital Personal Data Protection Act, 2023, and address various aspects, including safeguarding children's data, managing consent, transferring personal data overseas, and establishing a Data Protection Board, among other measures.

Schedules

- 1

Specifies the requirements for registering Consent Managers and their responsibilities.
- 2

Defines the standards for the State's processing of personal data.
- 3

Lists timeframes for data retention by certain categories of Data Fiduciaries.
- 4










Provides exemptions for processing children's personal data.
- 5

Details the terms and conditions for the appointment and service of the Chairperson and Members of the Data Protection Board.
- 6

Outlines the terms of service for the Board's officers and employees.
- 7

Identifies authorized individuals for specific functions under the Act.

Key Provisions and Main Factors

 Notice and Consent Data Fiduciaries must provide clear notices on data processing purposes and consent withdrawal options.	 Consent Management Registered Consent Managers facilitate giving, managing, withdrawing consent with record-keeping.
 Security Safeguards Data Fiduciaries must implement measures like encryption and access control to prevent breaches.	 Data Breach Notification Notify Data Principals and the Board of breaches within 72 hours
 Processing of Children's Data Requires verifiable parental consent for processing data of individuals under 18.	 Significant Data Fiduciaries Must conduct annual DPIAs, audits, and meet additional compliance obligations.
 Cross-Border Data Transfers Personal data transfers outside India require Central Government approval.	 Rights of Data Principals Includes rights to access, correct, erase personal data, and withdraw consent.
 Governance and Oversight The Data Protection Board ensures compliance, addresses grievances, and enforces penalties.	

DPDPA Rules Brief

- Rule 1: Specifies the short title, commencement, and timeline for compliance with the rules.

Rule 2: Provides definitions to ensure consistent interpretation aligned with DPDPA.

Rule 3: Mandates clear, detailed notices for data principals about data processing and their rights.

Rule 4: Outlines registration and obligations of Consent Managers, detailed in the First Schedule.

Rule 5: Allows State entities to process personal data for public benefits under Second Schedule standards.

Rule 6: Requires Data Fiduciaries to implement security safeguards like encryption and access controls.

Rule 7: Specifies breach notification procedures for data principals and the Board, regardless of harm.

Rule 8: Sets timelines for erasing personal data when no longer needed, as detailed in the Third Schedule.

Rule 9: Requires Data Fiduciaries to publish contact details or DPO information for inquiries.

Rule 10 & 11: Mandates verifiable parental consent for processing children's data and person with disability, with specific measures.

Rule 12: Provides exemptions for certain entities from rules on parental consent and behavioral tracking.

Rule 13: Imposes additional obligations on Significant Data Fiduciaries, including annual DPIAs and audits.

Rule 14: Details data principals' rights like access, erasure, and nomination of representatives.

Rule 15: Regulates cross-border data transfers under conditions set by the Central Government.

Rule 16: Exempts research and statistical processing from the Act if standards in the Second Schedule.

Rule 17-21: Covers Data Protection Board setup, including appointments, terms, and meeting procedures.

Rule 22: Details the process for appealing Board decisions to the Appellate Tribunal.

Rule 23: Allows the govt. to request information from Data Fiduciaries for purposes in the Seventh Schedule.

Enforcement Timelines for DPDP Act

13 November 2025



Rules 1, 2 and 17–21

- Extent & applicability
- Definitions
- Data Protection Board establishment
- Board powers & functions
- Investigation & adjudication
- Appeals to Appellate Tribunal

13 November 2026



Rule 4

- Registration and Obligations of Consent Managers

13 May 2027



Rules 3, 5–16, 22 and 23

- Notice, Consent and processing by State
- Reasonable Security Safeguards
- Intimation of breaches and data retention
- Contact information of DPO or equivalent
- Verifiable Consent for Child and PwD
- Obligations of Significant Data Fiduciary
- Data principal Right Management
- Cross Border Data Transfer


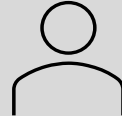
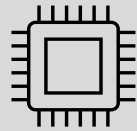
Key Obligations of Data Fiduciary

Key Data Fiduciary Obligations

01	Take consent from Data Principals where required and implement a Consent Management mechanism. (Section 4(1) of DPDPA 2023, First Schedule, Rule-3 and 4, DPDP rules 2025)	05	Review and update the grievance redressal mechanism for handling queries from data subjects. (Section 8(10) of DPDPA 2023, Rule-14(3), DPDP Rules 2025)
02	Provide a privacy notice to Data Principals at the time of providing consent for processing their personal data. (Section 5 of DPDPA 2023, Rule-3, DPDP Rules 2025)	06	Implement a process for receiving, acknowledging and honouring Data Principals Rights (Sections 11, 12, 13, & 14 of DPDPA 2023, Rule-14, DPDP Rules 2025)
03	Implement appropriate technical & organizational measures to safeguard personal data. (Section 8(4) of DPDPA 2023, Rule-6, DPDP Rules 2025)	07	Implement data retention & disposal mechanism in consonance with other laws. (Section 8(7) of DPDPA 2023, Rule-8 & Third Schedule, DPDP Rules 2025)
04	Sign a valid contract with your Data Processors / third parties to ensure key obligations are abided by. (Section 8(2) of DPDPA 2023, Rule-6, DPDP Rules 2025)	08	Implement a Data Breach management mechanism to notify Data Principals and Data Protection Board . (Section 8(6) of DPDPA 2023, Rule-7, DPDP rules 2025)

*Organization can qualify as 'Significant Data Fiduciary' based on the volume, sensitivity of personal data and risks to the rights of Data Principals.

Significant Data Fiduciary* Key Obligations

Data Protection Impact Assessment	 Conduct Data Protection Impact Assessment periodically
Data Protection Officer (DPO)	 Individual appointed to play the role of a DPO within India
Data Audits	 Perform data audits at regular intervals by an Independent Auditor

Changes that we foresee in NBFCs post DPDP's Mandate

A primer



Customer engagement – from lead generation, loan application, credit assessment, disbursement, EMI collection, servicing, cross-selling, to closure– all processes need to change



Partner engagement models may change leading to more insourcing or staff augmentation and less outsourcing



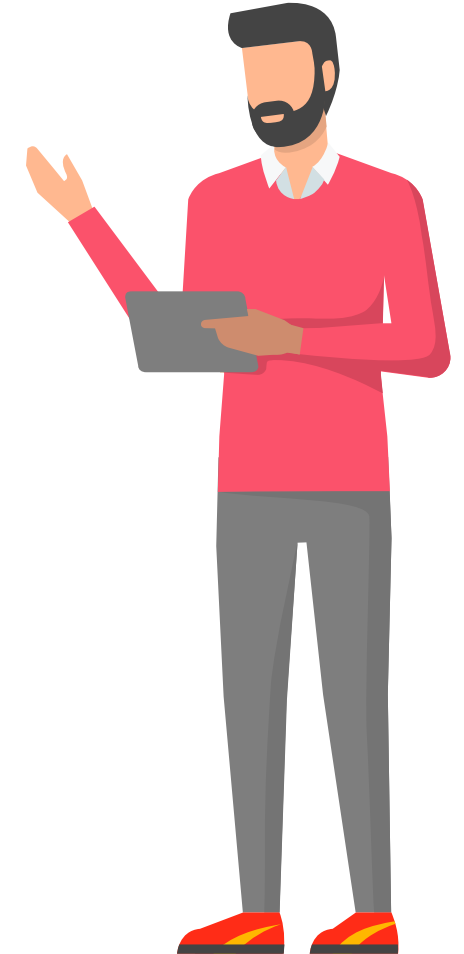
Data usage, technology and information security will need a significant re-thinking incorporating flags, consents, data archival, log monitoring, access controls etc.



Strategic decisions will have to be taken for extent of obtaining and using customer data including processing of child data



Customer rights management will need a separate function, team, processes and tech.



Why companies need to comply with DPDPA

The Data Protection Board of India can impose heavy penalties on companies (Data Fiduciaries) that mishandle personal data under the DPDP Act.

Up to Rs. 250 Cr

Upon failure to comply with data protection obligations (e.g. lawful processing, transparency, purpose limitation)

Up to Rs. 200 Cr

Upon failure to take reasonable security safeguards to prevent a data breach

Up to Rs. 200 Cr

Upon failure to notify the Data Protection Board and affected data principals of a data breach.



Up to Rs. 150 Cr

Upon Non-Compliance with additional obligations of significant data fiduciaries (e.g. data audits, appointment of DPO)

Up to Rs. 200 Cr

Upon Violation of children's or Persons with Disability data processing rules

Up to Rs. 150 Cr

Upon non-fulfilment of data principal's rights (e.g., not providing access or erasure of data)

Few relevant use – cases for NBFCs



Consumer Durable Loans and On spot EMIs

Consumer durable loans and on-spot EMIs are approved within minutes once a customer's Aadhaar, PAN, and contact details are entered into the system.

What Changes -

NBFCs must embed a consent step in the EMI approval flow, ensuring customers explicitly agree to data use before processing begins



Housing Finance

Home loans are **long-term financial products** requiring extensive personal and property data collection, often retained for years.

What Changes-

Companies must embed a consent solution in the home loan workflow before processing applicants' personal data.

NBFCs should build workflows to handle data principal rights requests like data correction.



Education Loan

Education loans often involve collecting personal data of students, including academic records and guardian details—**especially when the applicant is a minor.**

What Changes -

If the student is under 18, companies must obtain verifiable consent from a parent or lawful guardian before processing any personal data.

Companies will have to ensure that no data processing is carried out that may cause detrimental effect on the well-being of a child.

Overall methodology for privacy program

Enterprise-wide privacy

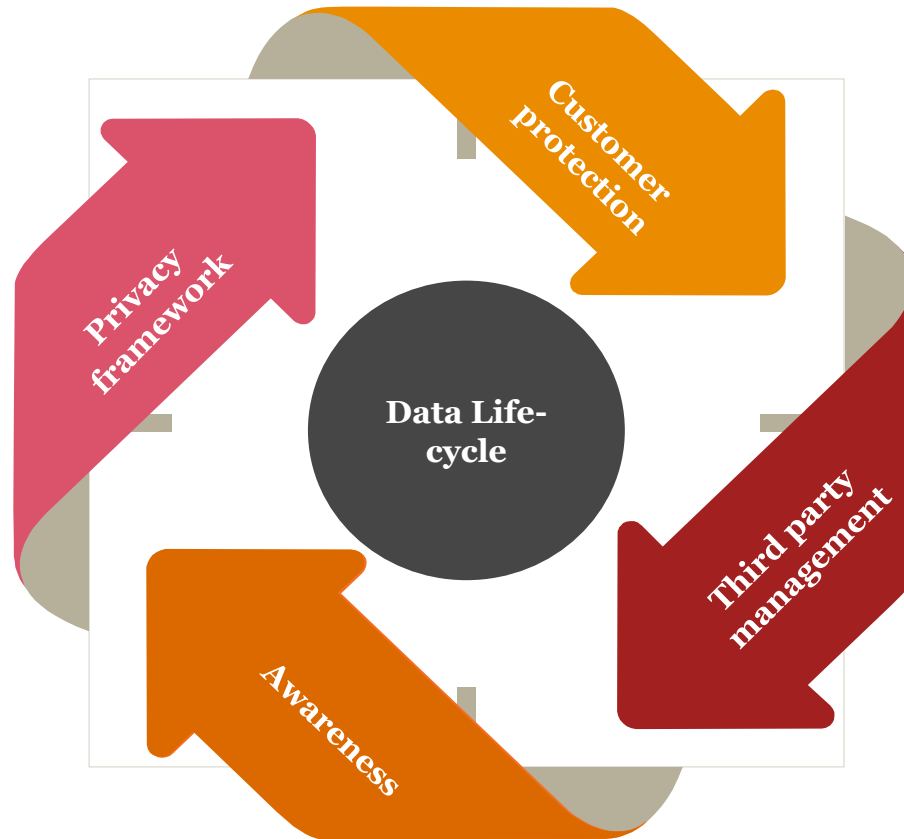
- Data privacy policy and frameworks
- Consent management framework process and system
- Privacy notice
- Personal data breach management and notification

- Integration with legal for consent / notice
- Alliance with privacy tool
- Integration with ERM

Educating employees, vendors and contractors

- Privacy org. design
- DPO / DPO team setup
- Privacy awareness – internal and external
- Communications management

- Global privacy org & R&R
- Skillsets on DPO teams (i.e. CIPP etc.)
- Alliance with privacy content creators



Customer data privacy and protection

- Data flow assessment and data inventory
- Privacy / Data discovery tool implementation
- Business process re-design incl. PbD and consent
- IT architecture
- IS tools management

- Integration with business process teams
- Consent / Notice execution skills
- Skillsets on DLP and IRM

Third party privacy risk management

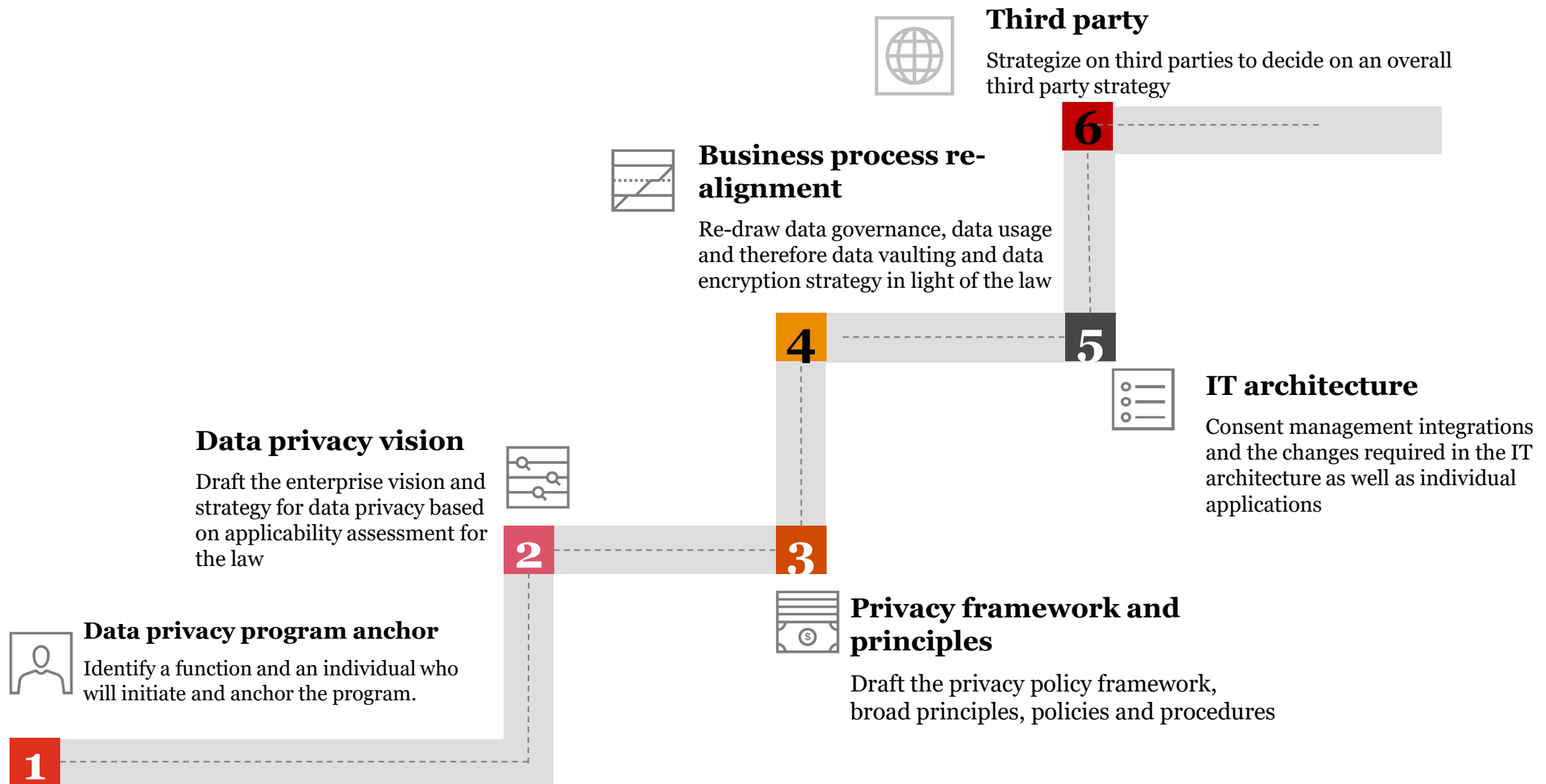
- Critical vendor inventORIZATION
- Vendor contract redrafting
- Vendor security measures implementation
- Vendor ongoing risk assessments

- Integrated tool based third party risk management

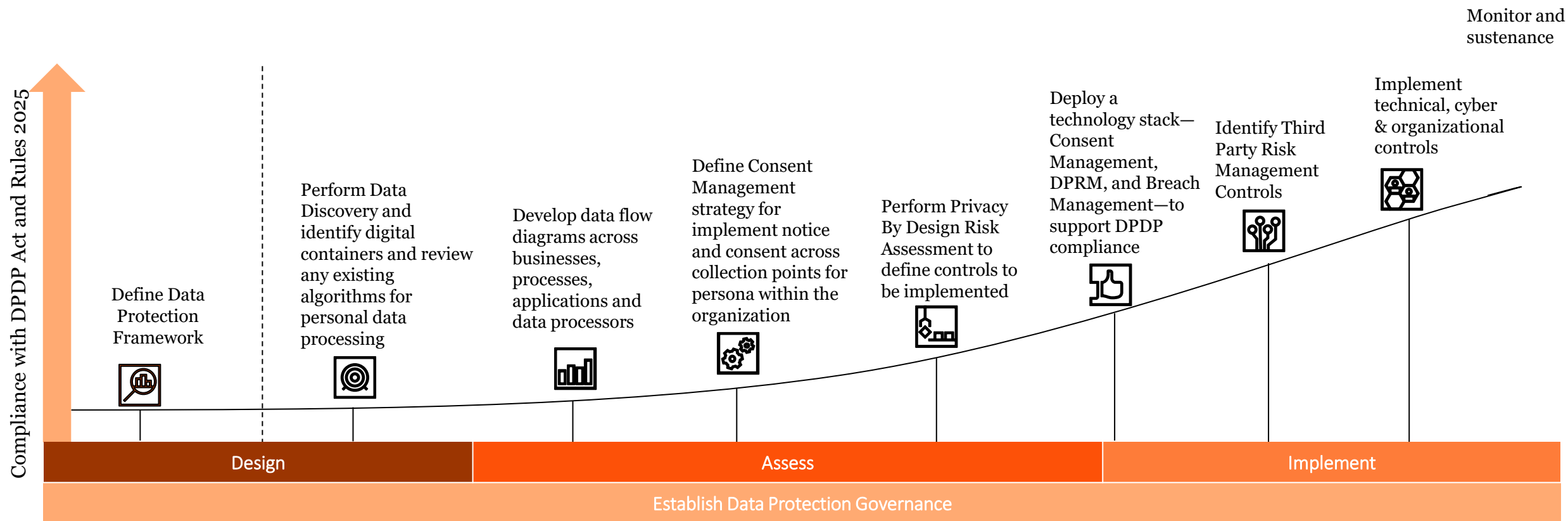


Initial steps

Here is PwC's Point Of View (POV) on approaching data privacy implementation program. Based on the below approach, we have crafted an approach for NBFCs



Summary of Overall Project Approach



PwC brings a deep data protection and privacy experience across all phases

An Overview of Privacy Tools



November 2025

Overview of leading global PETs and what they have to offer



While PwC is a tool agnostic organization; here is an overview of some Privacy Enhancing Tool (PETs) and their capabilities.

Company	Consent Management	Cookie Management	Data Principal Rights Management	Compliance Management (DPIAs)	Third-party Risk Management	Personal Data Discovery & Inventory	Data Flow Diagrams	Data Minimization	Privacy Training Systems
Ardent	✓		✓	✓		✓	✓	✓	✓
Securiti	✓	✓	✓	✓	✓	✓	✓		✓
Seqrite		✓	✓			✓			
IDFY	✓	✓	✓	✓		✓	✓	✓	✓
Microsoft			✓	✓		✓	✓		
One Trust	✓	✓	✓	✓	✓	✓	✓	✓	✓
Data Safeguard	✓		✓	✓		✓			

Legend:



Capability exists



Capability partially exists



Capability does not exist

Questions



November 2025

Question #1



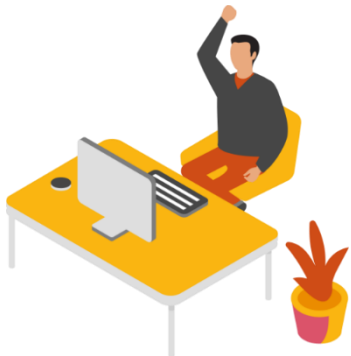
Your marketing team wants to use loan applicant data to promote unrelated insurance products. What principle of DPDPA does this violate?

A. Data minimization

B. Purpose limitation

C. Storage limitation

D. Accuracy



Question #2



A customer who closed their loan account with your company two years ago requests that their personal data be deleted from your systems. What is your company's obligation under DPDPA?

A. Retain the data for future marketing

B. Delete the data unless legally required to retain it

C. Refuse the request as the loan was closed

D. Archive the data indefinitely for audit purposes



Question #3



Your NBFC discovers a data breach involving customer loan records. What is your first obligation under DPDPA?

A. Inform the customer only if they complain

B. Delete the affected data immediately

C. Notify the Data Protection Board and affected data principals

D. Wait for internal investigation to conclude



Thank You