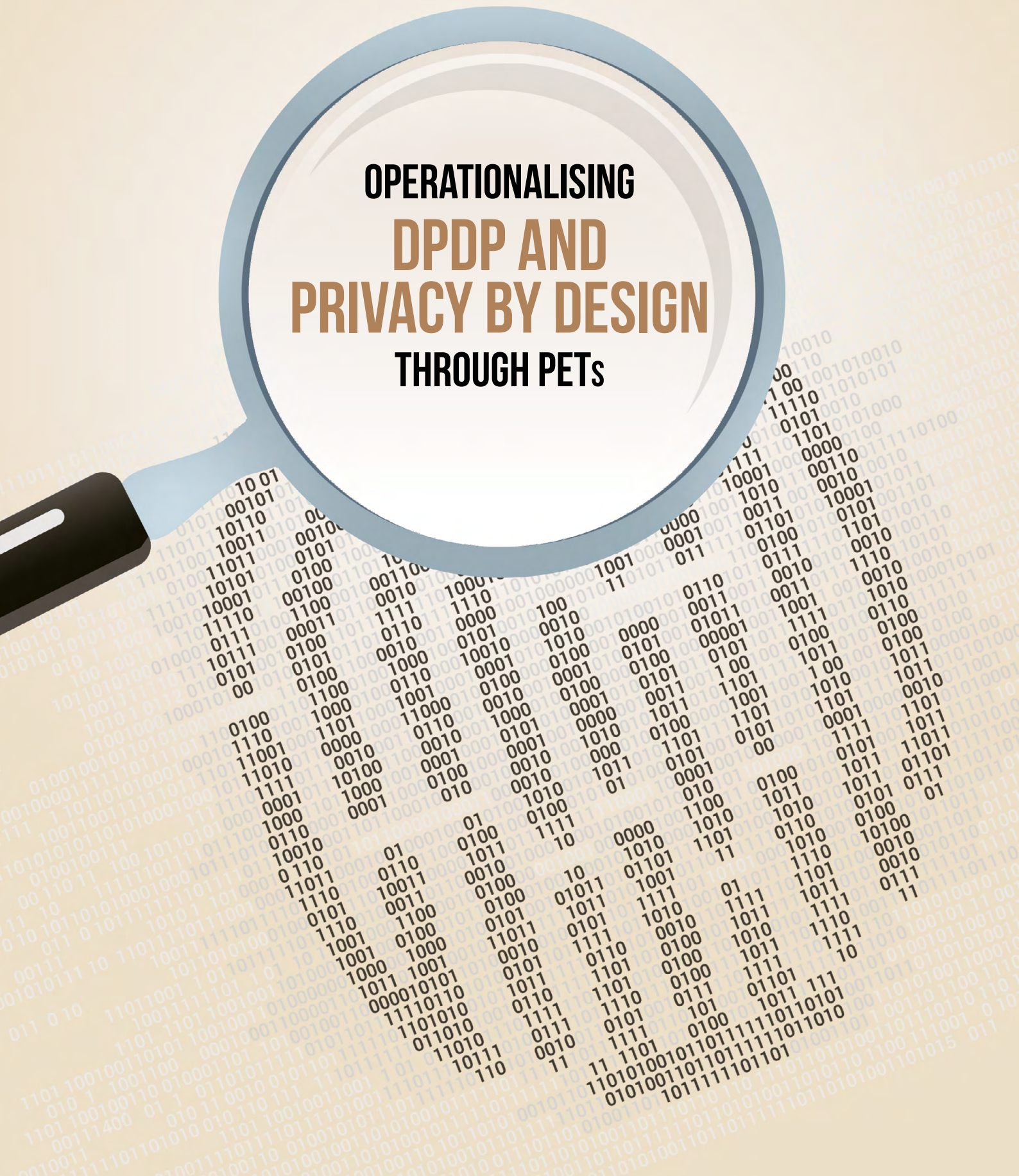
PrivaSapien
Evolution for the Privacy & AI Era

DSCI
PROMOTING DATA PROTECTION

OPERATIONALISING DPDP AND PRIVACY BY DESIGN THROUGH PETs



CONTENTS

EXECUTIVE SUMMARY

Upon the enforcement of the Digital Personal Data Protection Act, 2023, and the Digital Personal Data Protection Rules, 2025 (DPDP framework) in November 2025, India now needs an approach where data protection is not a mere compliance exercise but a design element before commencing any data processing. Due to the nascent nature of the DPDP framework, organisations may face difficulties turning legal compliance into demonstrable compliance. As Artificial Intelligence (AI), cloud-native systems, and interconnected platforms continue to grow, digital personal data offers both significant strategic value and material privacy risks to individuals' rights. Under this backdrop, the Data Security Council of India, with support from Privasapien, envisaged the thought of putting together this white paper, which may provide diverse stakeholders an opportunity to practically implement the DPDP Act within their organisation, providing a practical, techno-legal roadmap along with sectoral use cases for operationalising Privacy by Design (PbD) and Privacy-Enhancing Technologies (PETs) in alignment with the DPDP framework and international standards.

THE GROWING COMPLEXITY OF DATA ECOSYSTEMS UNDERSCORES THE NEED FOR GOVERNANCE APPROACHES THAT DO NOT MERELY REACT TO PRIVACY HARMS BUT PROACTIVELY EMBED PRIVACY PROTECTIONS INTO THE DESIGN AND DEPLOYMENT OF TECHNOLOGIES.

The white paper supports the idea that a design-led approach to the DPDP framework may transform data protection from a compliance obligation into a strategic business advantage by reducing breach liability, strengthening institutional trust, and accelerating enterprise adoption. It distinguishes privacy and data protection from cybersecurity, noting that security protects against unauthorised access while privacy governs whether authorised data use is lawful, proportionate, and purpose-bound. Using the Privacy Triad of Disassociability, Predictability, and Manageability, along with a case study, the white paper shows that many consent failures are architectural issues that require technical solutions, such as Consent-Based Access Control (CBAC). It further maps privacy risks across the data and AI lifecycle through Privacy Threat Modelling (PTM) and examines Privacy-Enhancing Technologies (PETs), including pseudonymisation, differential privacy, federated learning, synthetic data, and confidential computing, as tools that reduce personal data exposure while preserving analytical utility and supporting compliance with DPDP exemptions for research and statistical purposes.

Building on this foundation, the paper proposes an integrated four-stage PbD framework comprising lawful purpose and consent definition, PTM-based risk assessment, Data Protection Impact Assessments (DPIAs), and enforcement through CBAC and PETs. It also applies this framework across India's sectoral landscape through use cases, while drawing lessons from the European Union, the United Kingdom, California, and Singapore on embedding PbD and PETs into enforceable yet innovation-friendly regulatory systems. The white paper concludes that traditional notice-and-consent models are inadequate when privacy is not embedded in the system architecture from the outset, and that many privacy failures arise not from weak security but from processing that exceeds consent, purpose, or a lawful basis. Effective DPDP compliance, therefore, depends on integrating lifecycle mapping, PTM, DPIAs, CBAC, and PETs into a unified governance architecture that enables both meaningful protection and responsible innovation.

Furthermore, the white paper provides policy recommendations for industry stakeholders, regulators, and the government. Industry stakeholders may adopt cross-functional privacy governance with clear authority over consent management and DPIAs for high-risk processing, particularly with health, financial, or AI datasets. Implementing CBACs and PETs according to data-flow risks can support durable compliance. For regulators and the government, a baseline technical guidance framework could be developed to map data protection obligations to specific controls, distinguishing between Data Fiduciaries and Significant Data Fiduciaries. Creating interoperable accountability frameworks and harmonising anonymisation standards can help prevent regulatory arbitrage. The Data Protection Board may recognise PET deployment as a mitigating factor in enforcement, encouraging the adoption of privacy technologies. Additionally, capacity-building measures, such as privacy engineering curricula across various disciplines, could help address India's implementation capacity deficit.

The overarching direction is clear: privacy governance in India's digital economy is to be operationalised, measured, and enforced across the full data and AI lifecycle, not confined to legal departments, but embedded across systems, institutions, and sectors.

INTRODUCTION
INDIA'S PRIVACY INFLECTION POINT

Safety accelerates innovation. No one uses a vehicle without controls such as a clutch, brake, or steering wheel. In the similar vein, as we enter the Artificial Intelligence (AI) era, it is critical for humanity to have the right controls in place before accelerating towards emerging technologies. Humankind's pursuit of efficiency and an improved quality of life have been reflected in technological innovations. Technology has reshaped social interaction, economic activity, and governance, leading to the Information Age of the late twentieth century. Innovations such as high-speed computing, global connectivity, and widespread digitisation have transformed the creation, storage, processing, and sharing of data, enabling greater access to digital services and data-driven decision-making.[1]

Personal data has become a critical strategic asset enabling personalised services, operational efficiencies, and innovation across sectors in today's digital economy.[2] As organisations adopt emerging technologies such as AI and quantum computing, gaps in traditional data protection become evident. The volume of personal data and the sensitivity associated with it have increased the risk of violating one's fundamental right to privacy,[3] along with concerns about data misuse, opaque processing, function creep, and pervasive surveillance.[4] The growing complexity of data ecosystems underscores the need for governance approaches that do not merely react to privacy harms but proactively embed privacy protections into the design and deployment of technologies.

THE GROWING COMPLEXITY OF DATA ECOSYSTEMS UNDERSCORES THE NEED FOR GOVERNANCE APPROACHES THAT DO NOT MERELY REACT TO PRIVACY HARMS BUT PROACTIVELY EMBED PRIVACY PROTECTIONS INTO THE DESIGN AND DEPLOYMENT OF TECHNOLOGIES.

Privacy by Checklist vs Privacy by Design

The traditional approach of "privacy as a cost centre" and, hence, "privacy by checklist"[5] treats compliance as a finite list of boxes to check: publish a notice, collect consent, appoint a Data Protection Officer, and file breach reports. Under India's Digital Personal Data Protection Act, 2023 (DPDP Act), this satisfies the letter of the law: notices,[6] consent,[7] and Data Fiduciary[8] obligations,[9] but stops at minimum viable legality. It is reactive, audit-driven, and fragile.

Privacy by Design (PbD) embeds protection into systems from inception: data minimisation, purpose limitation, and security safeguards[10] built into architecture, not bolted on. It anticipates Consent Manager[11] flows, Data Principal[12] rights, and breach resilience proactively. The DPDP framework rewards this; the genuine accountability reduces enforcement risk and operationalises consent rather than merely documenting it.

Approaches such as PbD and Privacy Enhancing Technologies (PETs), when coupled with law, have emerged as critical safety guardrails to protect privacy while unlocking data, which is essential for innovation. PbD emphasises the proactive integration of privacy safeguards throughout the system lifecycle, while PETs provide technical tools, such as data minimisation techniques, anonymisation, secure computation, and decentralised processing, that reduce personal data exposure without undermining innovation.[13] Together, these techno-legal measures enable organisations to balance economic value creation with the protection of individual rights.

PbD becomes a profit centre when protection is reframed as a product capability rather than a regulatory overhead. Under the DPDP framework, PETs help meet the exemption requirements to unlock data, baked-in data minimisation, and purpose limitation which cuts storage costs, breach liability, and audit costs, leading to measurable savings. Moreover, the upside is larger: privacy-native architecture accelerates enterprise sales cycles, where procurement and security reviews otherwise stall deals for months. It unlocks regulated markets closed to weak-compliance vendors, commands premium pricing, and shortens consent-driven onboarding into a frictionless funnel. Trust becomes a differentiator that competitors cannot retrofit inexpensively .

The Digital Data Protection Act, 2023: Technical Safeguards as the Highest Priority

Legislative frameworks play a critical role in translating these governance expectations into enforceable obligations. India's DPDP Act adopts a rights-based approach centred on lawful purpose, consent, data minimisation, and accountability of data fiduciaries.[14] The DPDP Act places direct, legally binding duties on Data Fiduciaries, and not mere aspirational principles. It also requires implementing appropriate technical and organisational measures to ensure effective observance of the DPDP framework and to protect personal data in possession or control, including reasonable security safeguards such as encryption, obfuscation, masking, or virtual tokens.[15] The stakes for non-compliance are considerable, with penalties of up to INR 250 crore under Schedule I of the DPDP Act.

Effective implementation of the DPDP framework, therefore, requires moving beyond policy documentation towards embedded, technology-driven privacy practices. Sustainable data governance requires integrating privacy into systems, processes, and decision-making from the beginning. Moreover, India's DPDP Act is a modern data protection regulation, where the highest priority and penalty is accorded to having technical safeguards to prevent breaches of personal data.

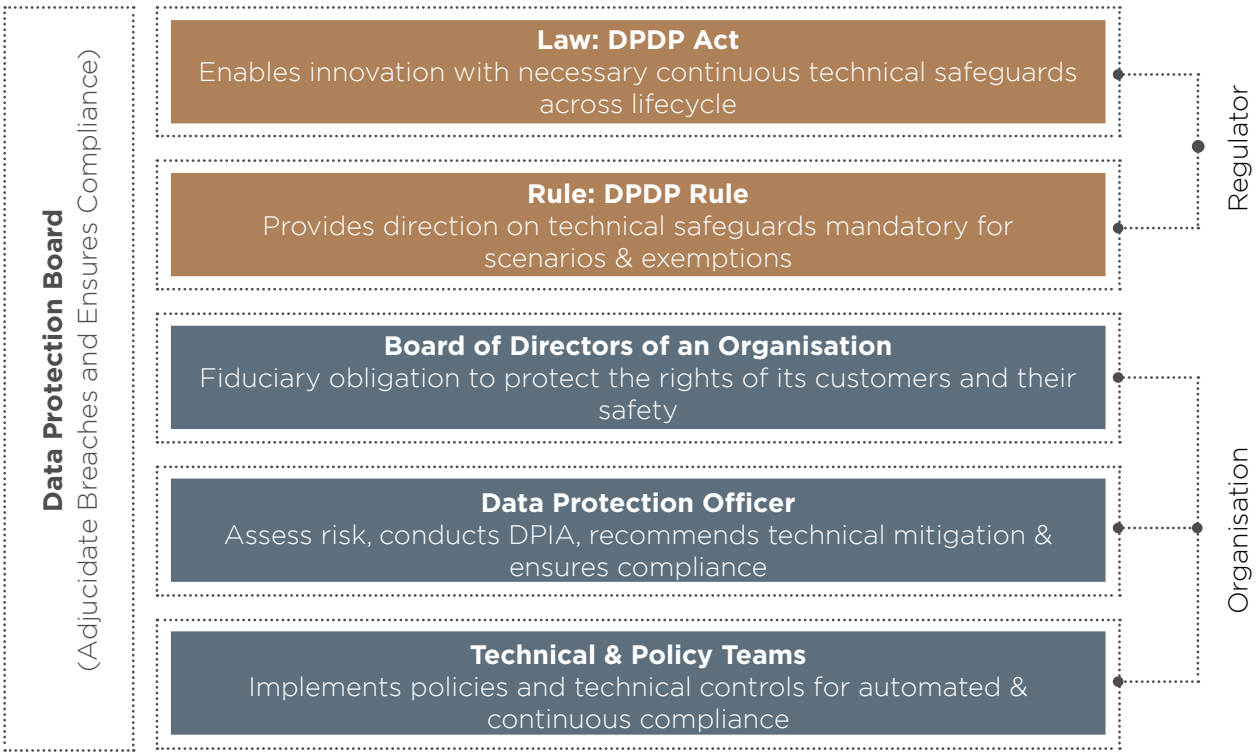


Figure: Provides a perspective of how the DPDP framework, the Board of Directors of an organisation, the Data Protection Office (DPO) and technical teams are given clear roles and action across the data lifecycle as per the DPDP Act, and breaches are adjudicated by the Data Protection Board to ensure compliance.

This white paper, therefore, seeks to bridge the widening gap between data protection law and its technological implementation. It examines how PbD and PETs may serve as practical instruments for operationalising data protection through technical safeguard obligations, while allowing data to be unlocked with exemptions when the data is personal, with particular focus on the DPDP framework. Rather than treating privacy as a documentation exercise or a post-incident compliance function, the white paper advances a design-led, technology-embedded approach to governance. It provides a horizontal, sector-agnostic framework that enables organisations across industries to integrate privacy safeguards directly into system architecture, engineering processes, and data lifecycle management.

The timing of this shift is critical as the rapid acceleration of technological innovation, particularly AI-driven systems, cloud-native infrastructures, and interconnected digital platforms, coincides with the operationalisation of modern data protection regimes. Organisations are no longer operating in a regulatory vacuum, and privacy cannot remain confined to legal departments. The coming years will determine whether privacy is experienced as a recurring compliance burden or leveraged as a strategic enabler of trusted digital growth. However, many enterprises face a persistent implementation challenge despite increasing regulatory clarity and organisational awareness: translating high-level privacy principles such as purpose limitation, data minimisation, accountability, and consent, among others, into

scalable, technology-enabled practices that function across diverse sectors and use cases.

In practice, organisations often:

- Understand statutory obligations but lack alignment between legal, engineering, and product teams;
- Conduct discovery from a security perspective, but miss the privacy perspective;
- Invest significantly in cybersecurity controls while underinvesting in privacy engineering capabilities;
- Conduct compliance assessments yet struggle to redesign legacy systems or embed privacy into new architectures;
- Consider and get misled that basic masking and encryption are PETs;
- Continue to view privacy primarily as a legal exposure rather than a foundational system design principle.

This white paper responds to that structural gap. It provides a practical roadmap for embedding PbD, a concept formalised in ISO 31700:2023[16] (the first international standard that defines requirements for integrating privacy across the lifecycle of consumer goods and services) and ISO 20889:2018[17] for deploying PETs, thereby enabling organisations to transition from reactive compliance management to proactive privacy governance. By systematically reducing unnecessary data exposure and integrating privacy into technical decision-making, organisations can simultaneously meet regulatory obligations, mitigate operational risks, and strengthen trust in this digital economy.

PRIVACY VS SECURITY
FOUNDATIONAL CONCEPTS AND THE LEGAL CONSTRUCTS

Privacy protects data in use (the purpose), while security protects data in rest and transit (the access). Once a person X downloads certain data after authentication, security cannot control what purpose they may use it for. Still, privacy can change the DNA of data, for instance, by generating synthetic data with PETs to prevent data breaches or the inappropriate use of personal data. Understanding this is at the very foundation of an organisation's privacy journey and is therefore important.

Architecting PbD systems and implementing PETs require clear concepts and alignment across sectors to apply data protection laws effectively. While these laws outline necessary privacy principles, technologies can help integrate concepts such as data minimisation and transparency into organisational practices and system architecture, making privacy by design and default operational with mathematical guarantees in the privacy implementation.

THE PRIVACY TRIAD, WHICH FOCUSES ON "DISASSOCIABILITY, PREDICTABILITY, AND MANAGEABILITY", COMPLEMENTS THE SECURITY TRIAD'S EMPHASIS ON "CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY", AS CODIFIED IN FRAMEWORKS SUCH AS ISO/IEC 27001 AND THE NIST CYBERSECURITY FRAMEWORK (NIST CSF).

This chapter outlines key constructs to connect law, governance, and engineering. It also distinguishes privacy from security, introduces proactive privacy risk modelling, maps the data lifecycle, and addresses the regulatory importance of data in use.

Privacy and Security – An Overview

The concepts of privacy and security are often used interchangeably in day-to-day discussions. Despite their close association, privacy and security have distinct uses and objectives, and are governed by different principles, obligations and risk considerations.

Security, in particular, information security, focuses on protecting information and information assets from unauthorised access, disruption, alteration, or destruction.[18] Privacy, in contrast, concerns the lawful, fair, and proportionate processing of personal data. It addresses normative questions such

as whether data should be collected, the purpose of data collection, whether the data collection is proportionate to that purpose, the data retention period, and what rights an individual has in relation to the data.[19] Under the DPDP Act, privacy obligations also extend beyond implementing reasonable security safeguards[20] to ensure lawful processing, purpose specification, consent management, and erasure upon withdrawal of consent.[21]

The diagram below provides a concise comparison of these concepts, highlighting the principal distinctions in their scope and application.

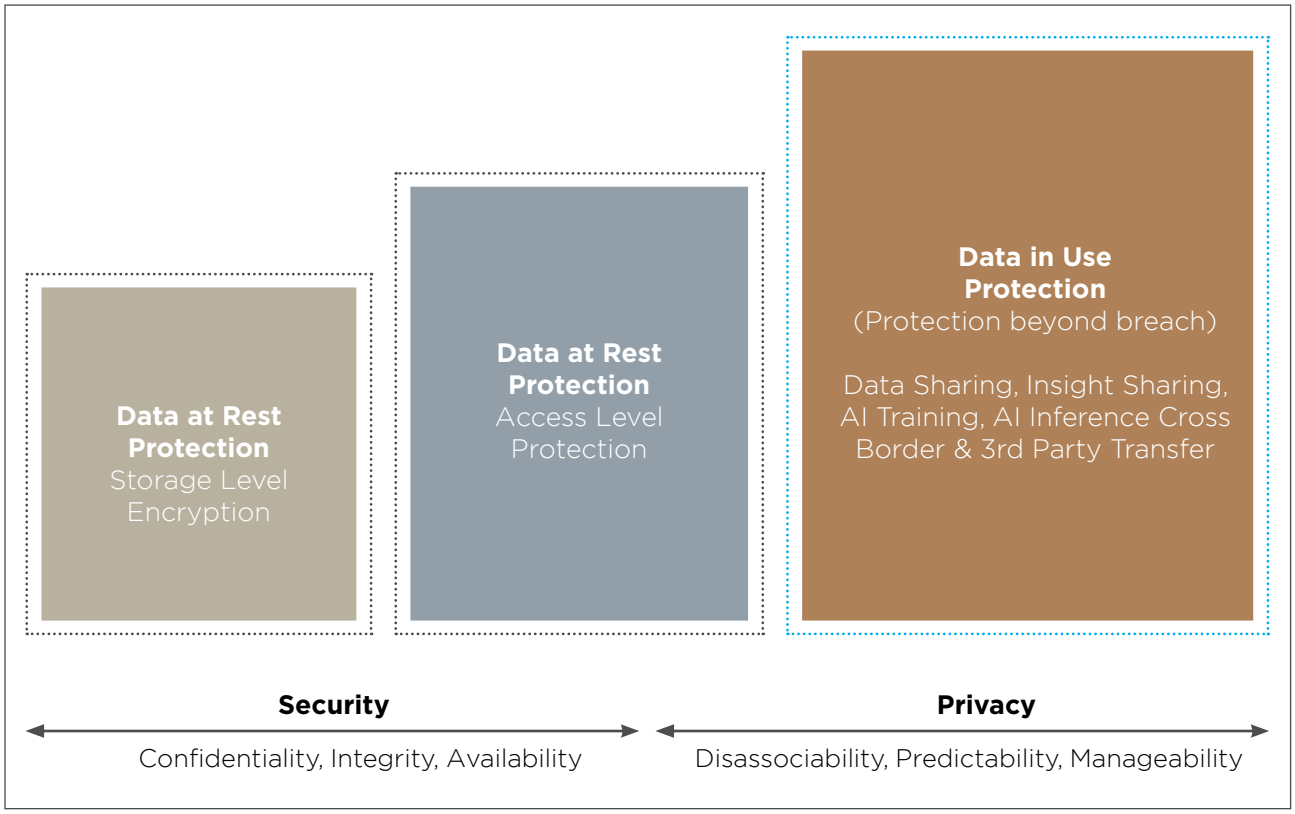


Figure: Distinction between Privacy and Security, and its application to data protection.

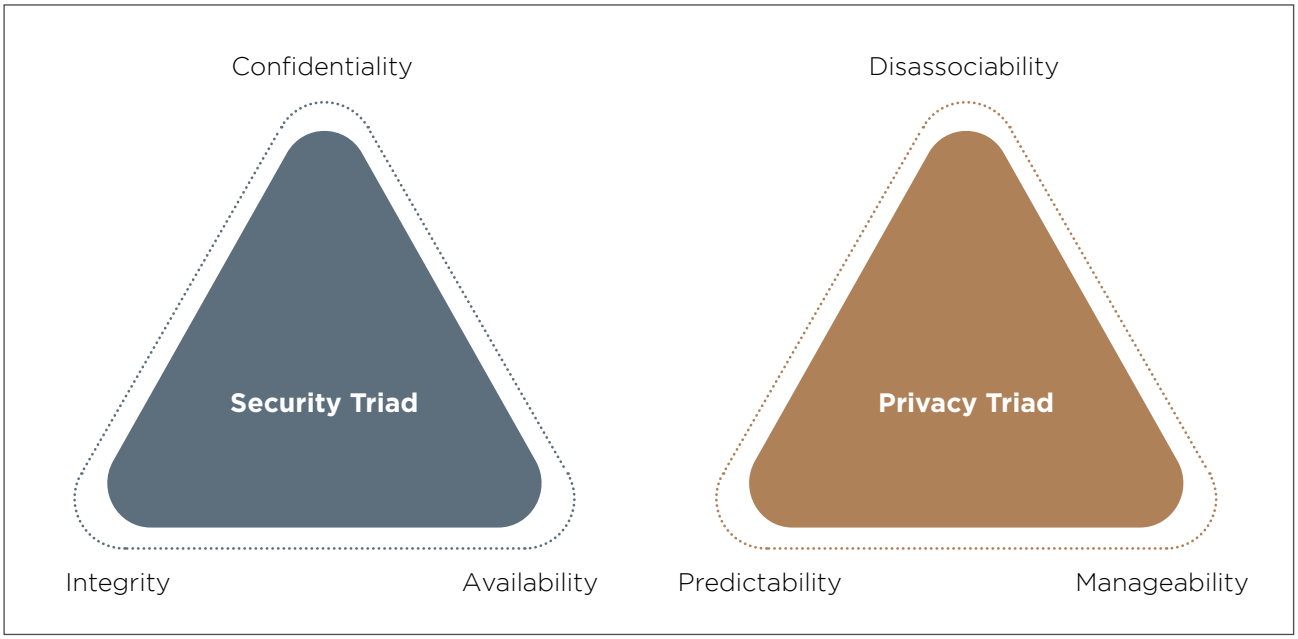


Figure: Pillars that comprise the Security Triad and the Privacy Triad.

Privacy and security are linked but have different goals. Security measures like encryption protect data at rest for compliance, but do not address privacy risks that arise when data is in use, such as misuse or re-identification of individuals during sharing and AI training. The Privacy Triad, which focuses on "Disassociability, Predictability, and Manageability", complements the Security Triad's emphasis on "Confidentiality, Integrity, and Availability", as codified in frameworks such as ISO/IEC 27001[22] and the NIST Cybersecurity Framework (NIST CSF)[23].

Privacy frameworks such as the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,[24] ISO/IEC 27701,[25] and the National Institute of Standards and Technology's (NIST) Privacy Framework (NIST PF)[26] expand governance beyond security controls to include transparency, purpose limitation, individual participation, and accountability. Therefore, security protects data from unauthorised access, while privacy safeguards individuals from harm arising from authorised use of data. This distinction between privacy and security often complicates translating broad privacy policies into specific system requirements.

i. Privacy Triad – Disassociability, Predictability, and Manageability

NIST's Internal Report 8062 (NISTIR 8062) addresses the challenge of operationalising the Privacy Triad and translating policy intent into system-level engineering objectives. The NISTIR 8062 frames "Disassociability, Predictability, and Manageability" as design imperatives to guide system engineers in implementing controls to manage privacy risks at the data-in-use stage.[27]

Dimension of Privacy Triad	Concept	Link to the DPDP Act	Operational Implications
Disassociability	Addresses risks arising from the Data in Use stage; focuses on separating identity from data within authorised environments, rather than restricting access.	Section 17(2)(b) of the DPDP Act provides an exemption for research, archiving, or statistical purposes if the personal data, which is neither identifiable nor relatable,[28] is also considered to be a reasonable security safeguard for consented and continued processing.[29]	Requires systems to minimise any potential exposure of a user/individual's identity during data processing, using PETs that can provide mathematical guarantees of acceptable levels of dissociation, which may be recommended for the data flow during a Data Protection Impact Assessment (DPIA).[30]
Predictability	Enables users/ individuals to form reliable expectations about how their personal data will be processed and disclosed, and at what level of personal data will be processed and disclosed, that is, identifiable and relatable.	Data Fiduciary must conduct periodic risk assessments[31] of the level of identifiable and relevant personal data being used and provide a summary of the personal data being processed.[32]	Systems must support predictable risk quantification and the relatability of personal data, and provide a summary of such processing to the Data Principal.[33]
Manageability	Allows the exercise of a Data Principal's rights, enabling granular data administration through technical measures, including collection, alteration, deletion, and selective disclosure.[34]	Stems from Chapter III of the DPDP Act, which governs the rights and duties of a Data Principal,[35] which requires Data Fiduciary administration to manage and provide a summary of processing activities,[36] along with technical safeguards used[37] for processing of personal data and continuous processing.[38]	Data Fiduciary has to manage the personal data processing by understanding the risks associated with the requested data, mitigating them with technical safeguards such as PETs, approving such data flows, and summarising the list of such personal data processing to customers.

Table: Mapping the Privacy Triad Dimensions to the DPDP Act and Their Operational Implications

ii. Overlaps and Interdependencies

Privacy and security often overlap to ensure that a system is end-to-end secure. In today's data-centric digital economy, maintaining trust and protecting sensitive data rely heavily on privacy and security as interrelated facets of information management. The following highlights their commonalities:

- Both privacy and security aim to protect sensitive personal information from unauthorised access or misuse.
- The integration of both aspects is essential for fostering and sustaining trust in an organisation's initiatives, particularly those within the digital landscape.
- Robust data security measures contribute to privacy protection by establishing more formidable barriers against unauthorised access to personal information.[39]

At the same time, the NIST PF[40] clarifies that privacy and security are also structurally aligned with the NIST CSF[41] to enable organisational interoperability and integration within enterprise risk management systems. The framework adopts an 'identify–protect–respond' model and includes privacy functions such as control and communication to promote transparency and accountability.[42] It emphasises the need for cybersecurity measures, such as encryption and access controls, to support privacy safeguards. Additionally, privacy governance calls for organisations to evaluate the necessity and impact of their data-processing choices, positioning privacy as a risk-based governance discipline within system design, rather than just a subset of security.[43]

iii. Privacy by Design across the Data and AI Lifecycle

- Data, when collected from Data Principals, should be collected with the understanding of the obligations the data comes with, including consent[44], and provide Data Principals with rights granted by Chapter III of the DPDP Act.[45]
- Identify and manage a summary of personal data (not just personally identifiable information)[46] that is identifiable and relatable,[47] and processing activities by the Data Fiduciaries and identities of all other Data Fiduciaries and Processors[48] with whom the Data Fiduciary shares the personal data.[49]
- Conduct a DPIA[50] which comprises the purpose of processing of data,[51] quantification of risk of personal data, conduct the assessment of the purpose of processing, risk identified, recommend management and mitigation of risk with technical safeguards.[52] While Significant Data Fiduciaries (SDFs) must conduct a DPIA, all Data Fiduciaries (even those that would not be classified as SDFs) must comply with regulatory requirements to provide a summary of their personal data processing activities, along with appropriate technical safeguards and organisational measures.[53] This is a key governance step that is critical for controlling data and orchestrating technical safeguards across the organisation.
- Given that a Data Fiduciary has to process personal data as per consent or other grounds for processing, and is to be controlled with PET technical safeguards like consent-based dynamic encryption or masking, Consent-Based Access Control (CBAC) with dynamic encryption, data flow masking, or data sharing to internal and third-party ecosystems can help meet technical safeguards and organisational measures,[54] and protect data flows across the data lifecycle.

Governance Implications for Industry

The distinction and interdependence between privacy and security have important governance implications for industry. As organisations expand digital operations, privacy and security must be integrated into enterprise risk management, board oversight, product development, and regulatory compliance.

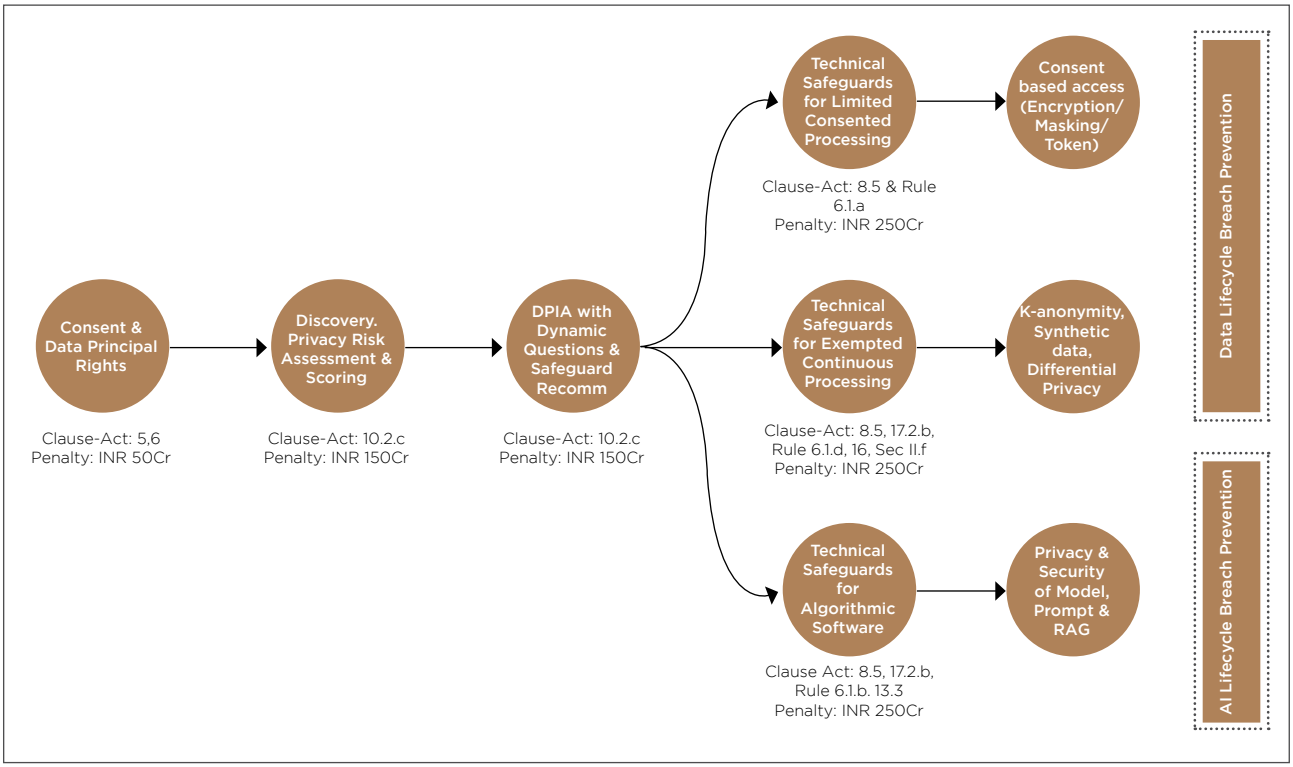


Figure: Privacy by Design across the Data and AI Breach Prevention

First, security programmes must incorporate data minimisation logic. Traditional cybersecurity prioritises data protection, while privacy governance encourages organisations to reconsider the need to collect personal data. This shift emphasises data minimisation, reducing the attack surface and aligning with principles like purpose and storage limitation. Businesses should, therefore, integrate minimisation criteria into system architecture, procurement, vendor onboarding, and AI training datasets, rather than applying security controls post-collection.[55]

Second, privacy governance must integrate technical safeguards at the design stage, rather than relying solely on policy documentation or post-deployment audits. Legal compliance typically comes into play post-deployment, but AI-driven and cloud-native platforms need integrated privacy controls from the start. This includes access controls, encryption, pseudonymisation, and accountability logging. Governance frameworks should promote collaboration among legal, engineering, product, and security teams, and standardise Privacy Impact Assessments, threat modelling, and lifecycle mapping in system design.[56]

Third, boards and regulators must avoid equating cybersecurity maturity with privacy compliance. An organisation may have advanced security measures but could still engage in excessive data collection, indefinite retention, or opaque profiling. Therefore, governance oversight should expand beyond cybersecurity metrics to include data inventory accuracy, retention practices, consent management, and alignment with stated purposes. This requires audit and risk committees to broaden their evaluation criteria.[57]

Thus, privacy should be viewed as a fundamental component of industry governance. It must be integrated into enterprise risk management, included in board oversight, and implemented through technology-driven safeguards.

To appreciate the governance implications, it is essential to move from principle to practice. The distinction between privacy and security, along with their interdependence in enterprise systems, affects how organisations design products, allocate budgets, manage risk, and ensure compliance. In India, the interplay between cybersecurity and data privacy is crucial, especially with the DPDP framework's emphasis on accountability. Compliance requires security measures and adherence to consent, purpose limitation, and erasure obligations. Many organisations confuse cybersecurity maturity with privacy compliance risks because their data governance is misaligned.

The following case study highlights how an organisation, initially confident in its security, faces challenges in integrating privacy into its technology and shows that aligning privacy engineering with cybersecurity strengthens both compliance and business resilience.

Case Study: The Consent that could not Travel

The Scenario

A retail bank's business team maintains customer records for account servicing — a lawful, consented purpose under the DPDP framework. To drive revenue, it shared a customer dataset with the marketing team for promotional offers and cross-selling. The marketing team ingested the data into its campaign ecosystem: CRM, email automation, and a dialler platform.

A customer received the first promotional email and immediately withdrew consent for marketing use, as is their right under the DPDP Act.[57] The business team logged the withdrawal. But the data had already been propagated into the marketing stack, including campaign lists, automation workflows, and cached segments. With no mechanism to propagate the withdrawal downstream, the campaigns continued. The customer received further promotional emails and cross-selling calls. He then escalated the matter and filed a complaint with the Data Protection Board (DPB).

Why This Is a Privacy Breach, Not a Security Breach

No system was compromised. No encryption failed. No unauthorised party accessed anything. Every system behaved exactly as designed, which is precisely the problem. The data was perfectly secure and simultaneously misused. The breach was deliberate: processing continued after the legal basis (Consent) for it had been revoked. Security had nothing to protect against here; this failure lived entirely in the privacy layer, where consent, not access, is the control.

The Solution: Consent-Based Access Control

The fix is architectural, not procedural. Consent state must become a real-time enforcement signal, not a logbook entry:

- Consent-based masking and encryption: When consent is withdrawn, the customer's personal identifiers are dynamically masked or cryptographically locked, rendering records non-actionable for marketing even if physically present in the ecosystem.
- Real-time consent propagation: Withdrawal triggers immediate enforcement across all downstream systems, inside and outside the organisation.

- DPIA integration: The DPIA maps every purpose to its consent dependency before processing is permitted.
- Outreach policy binding: Campaign execution checks live consent at send-time, not list-creation time.

Consent stops being documentation and becomes the access control itself.

Key Learnings from the Case Study

The case study illustrates a privacy failure that is not only acute but also one in which personal data flows beyond the system in which it was originally collected.

In enterprises, data is often shared with downstream processes and third parties, creating potential risks for unintended personal data disclosure. This can occur not through malicious attacks but due to structural gaps in data segmentation, scoping, and governance during transfers. A personal data breach may occur even if internal cybersecurity measures are in place, as data can be processed for purposes beyond consent or legal authorisation without adequate controls over its distribution, access, and duration. This is the structural gap that PbD and the framework set out in this white paper are designed to help mitigate.

RISK-BASED PRIVACY
DATA LIFECYCLE, THREAT MODELS, AND PRIVACY ENHANCING TECHNOLOGIES

Data today has become immensely significant, organisations need to manage it as both an asset and a liability, addressing its volume, velocity, variety, regulatory requirements, and security threats in today's complex data landscape.[58] Data processing requires a structured approach to governance. Effective data management now includes continuous risk identification, mitigation, and oversight throughout the entire data ecosystem, beyond just storage security and compliance.[59]

AI GOVERNANCE THROUGH TECHNO-LEGAL FRAMEWORK" (OPSA WHITE PAPER), STATES THAT DATA GOVERNANCE AND AI GOVERNANCE ARE INSEPARABLE.

This chapter discusses data lifecycle mapping and risk-based frameworks for responsible data management, focusing on control points and risks across the collection-to-deletion lifecycle. It promotes a dynamic risk assessment over static compliance checklists, allowing organisations to adapt to technological and regulatory changes. The chapter also introduces PETs like homomorphic encryption and differential privacy, which enable organisations to extract value from data while safeguarding individual privacy. It is observed that the adoption and use of PETs across the data lifecycle can help ensure that innovation, individual privacy, data protection compliance, and accountability evolve in tandem.

Data Lifecycle Mapping: Identifying Risks and Compliance Control Points

In today's digital landscape, personal data is constantly moving through various actors and systems from collection to deletion. Risks to data privacy may arise throughout this lifecycle, making it crucial for data-driven operations to understand and manage this journey. Understanding how personal data is collected, transformed, reused, and transferred is vital for identifying vulnerabilities, implementing safeguards, and ensuring accountability within organisations. This becomes much more crucial with the adoption, use and deployment of AI within organisations.

Data governance and AI governance now stand interconnected, and, in this regard, the Office of the Principal Scientific Advisor to the Government of India, in their white paper released in January 2026 titled "Strengthening AI Governance Through Techno-Legal Framework" (OPSA white paper), states that data governance and AI governance are inseparable.[60] The following is the Data and AI lifecycle identified in the white paper, which illustrates how personal data would flow from a business use to autonomous agentic-AI systems:

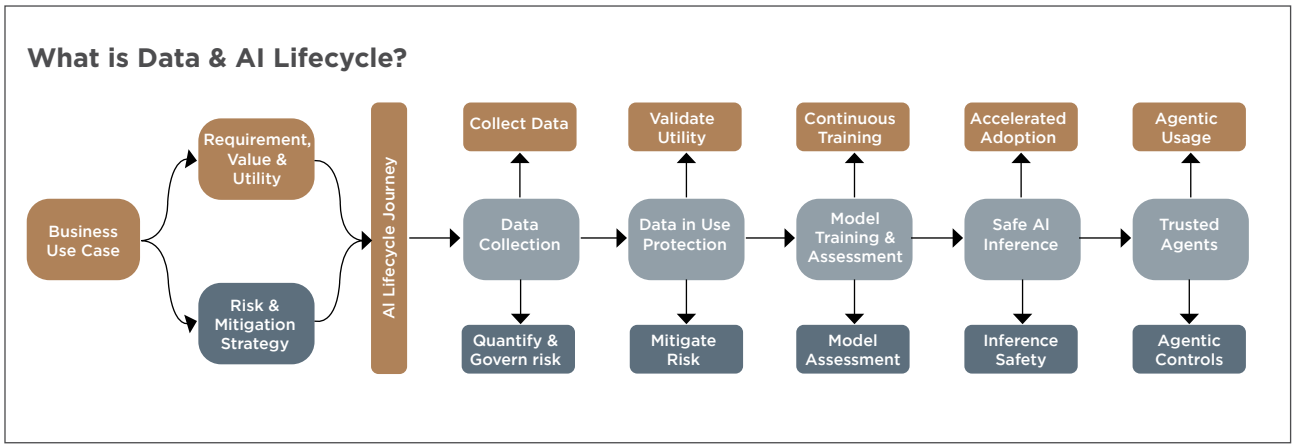


Figure: Data and AI Lifecycle depicted in white paper titled "Strengthening AI Governance Through Techno-Legal Framework"

The framework devised in OPSA's white paper establishes that two foundational pillars must be pre-defined before any activity in the data lifecycle:

- Firstly, requirement, value and utility articulating the purpose and proportionality of data processing, and
- Secondly, risk and mitigation strategies, which identify privacy threats, regulatory obligations, and safeguards at the design stage.

This reflects a broader principle, advocated by DSCI and endorsed by the OPSA white paper, that governance must be a design choice and not an afterthought. For organisations planning to be DPDPA compliant, this requirement directly translates into the obligations of lawful purpose, data minimisation, and consent management for Data Fiduciaries.

i. Data Lifecycle Mapping

Data lifecycle mapping is the foundational step for determining accountability and responsibility across the data value chain within an organisation. It enables organisations to understand where legal obligations attach and where governance controls must be embedded.[61] By making data flows visible and traceable, lifecycle mapping enables organisations to determine risk concentrations, assess compliance with privacy and security obligations, and design proportionate safeguards that remain effective throughout the data's operational lifespan.[62] Furthermore, robust data lifecycle mapping enhances data

protection and supports disaster recovery. There is a need for it, as during data lifecycle mapping, the associated privacy risks at each stage are identified, and governance and compliance measures are designed accordingly. From a data and AI lifecycle mapping perspective, the table below presents an illustrative list of risks for each stage of the lifecycle.

Stage of Processing/ AI Lifecycle	Associated Privacy and Security Risks	Safeguards
Data Collection	Over-collection Dark patterns Privacy risk Lack of governance	Notice[63] Consent[64] Data Minimisation[65] Privacy Threat Modelling (PTM) DPIAs
Data in Use Protection; Model Training and Assessment	Function creep Profiling Personal data breach No technical safeguards Data processing beyond consent or grounds for processing data	Purpose limitation[66] PETs Consent-based data flow control Reasonable security safeguards[67]
Model Training and Assessment	Model trained with personal data Vulnerable model deployed in production	Privacy-Preserved Machine Learning AI red teaming AI impact assessment
Safe Inference	Risk of privacy and security breach during interference Personal information flowing to the external model Sensitive data used for model training	Privacy and context firewall at the AI Interference level, with pseudonymisation interference protecting personal data against exposure
Trusted Agents	Hallucination Privacy and security breach in agentic use of data	Agentic red teaming Behaviour assessment Privacy, security and contextual firewalling of agents across the LLM and tool calling

Table: Data and AI Lifecycle Risks and Mitigation Safeguards

ii. Real-World Applications of Data and AI Lifecycle Mapping

In India, the DPDP Act imposes substantive obligations on Data Fiduciaries, including lawful collection, processing, and retention of personal data; obtaining informed consent for processing activities such as personalisation; adherence to the purpose limitation and data minimisation principles; and ensuring transparency in data-handling practices. Similarly, Data Principals are also provided rights to access, correct, erase, and withdraw consent,[68] necessitating corresponding updates across organisational data systems. Significant Data Fiduciaries (SDFs) are subject to enhanced compliance obligations, including the appointment of a Data Protection Officer, periodic audits, and impact assessments.

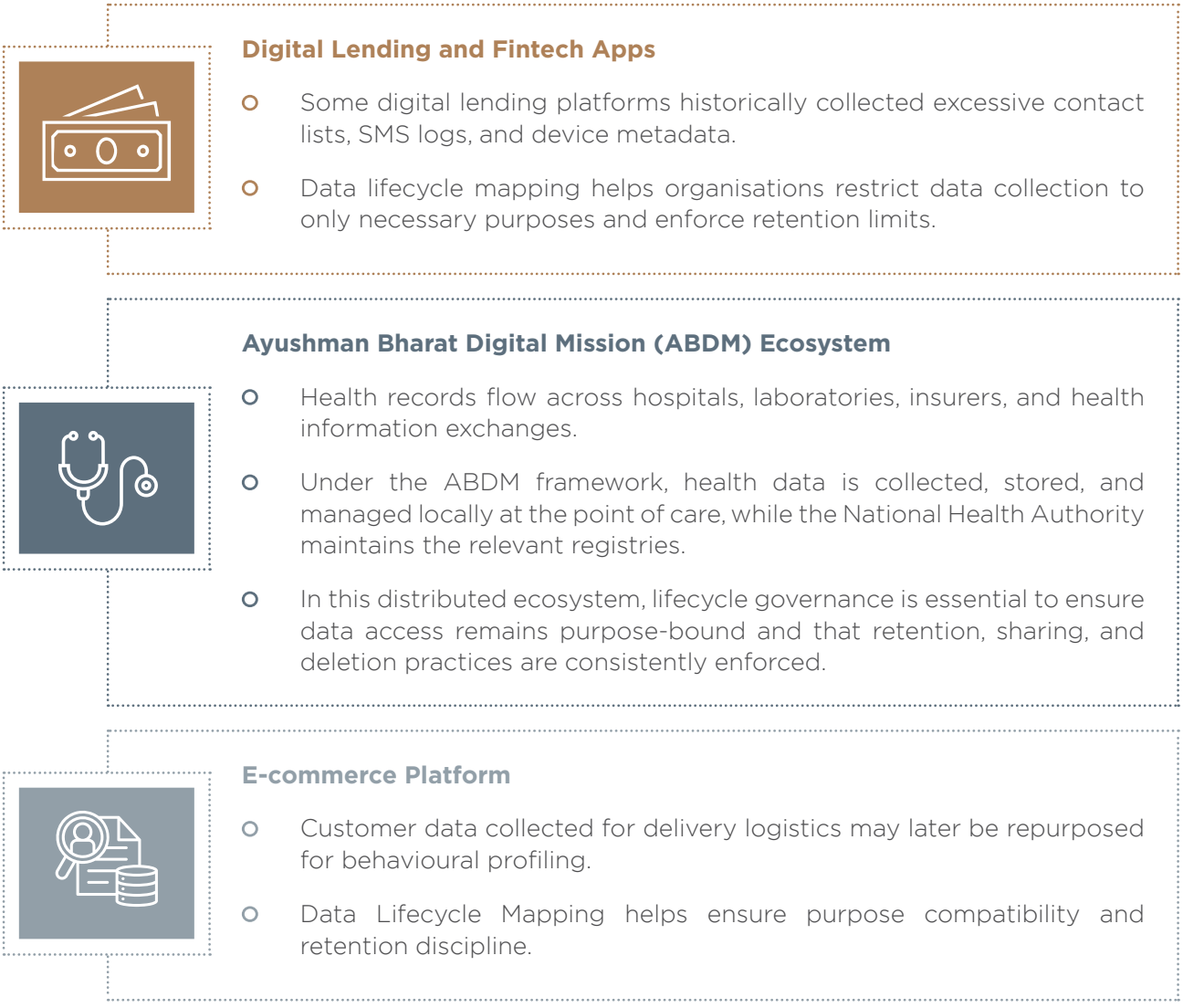


Figure: Sectoral Examples of Data and AI Lifecycle Mapping

In this context, effective Data Lifecycle Management (DLM) emerges as both a compliance imperative and a strategic governance mechanism. Embedding privacy and governance controls throughout the data lifecycle enables organisations to operationalise consent management, enforce purpose limitation, and comply with retention and erasure

obligations. Robust lifecycle governance further strengthens regulatory compliance, mitigates operational and reputational risks, and advances transparency and accountability, while enabling the PbD and PETs. Ultimately, disciplined data governance is essential for fostering trust and resilience in data-driven ecosystems.

Privacy Threat Modelling (PTM) and Data Security Posture Management (DSPM)

As discussed in the preceding chapters, privacy and security are complementary disciplines, not competing ones, a principle at the foundation of how DSCI has long approached governance through its parallel Security Framework (DSF) and Privacy Framework (DPF). Organisations building DPDP-compliant data governance should not choose between security posture management and privacy threat modelling; they need both, operating at different layers of the data governance stack, each doing what it was designed to do.

DSPM addresses the security layer: it tells an organisation where sensitive data resides, who can access it, and whether configurations and access controls meet security baselines. It is an essential foundation: without knowing where data lives, no privacy control can be reliably enforced. PTM addresses the privacy layer: it goes beyond access questions to ask whether data, even when accessed by authorised parties, is being used within the bounds of consent,[69] purpose,[70] and the Data Principal's reasonable expectations.[71]

i. Privacy Threat Modelling

PTM is a proactive PbD approach that identifies and evaluates potential privacy risks arising from how data is collected, processed, shared, and related across systems.[72] It focuses on data relatability, identifiability, and contextual risk,[73] thereby assessing how different data points, when combined, could lead to re-identification or misuse of personal information. The primary objective of PTM is to manage privacy risks before they materialise proactively. This involves:

- Detecting potential privacy vulnerabilities during system design and development.
- Evaluating the severity and likelihood of privacy breaches.
- Implementing mitigation strategies aligned with regulatory frameworks.
- Ensuring privacy principles are integrated into architecture and processes from inception.[74]

Key Characteristics

- Evaluation data flows and relationships between datasets.
- Consideration of purpose limitation, lawful basis, and data minimisation principles.
- Modelling threats to individual privacy, not just system security.
- Enabling preventive design controls, such as pseudonymisation, minimisation, and PETs.

i.a Frameworks for PTM

PTM encompasses data flows by tracking personal data movement, system components by reviewing applications and storage for privacy risks, and business processes by evaluating operational practices, third-party integrations, and cloud environments for compliance. Several established frameworks support organisations in effectively implementing PTM, which are as follows:

Framework Name	Core Concept	Operational Implications	Relevance to the DPDP framework
Linkability, Identifiability, Non-Repudiation, Detectability, Disclosure of Information, Unawareness, and Non-Compliance (LINDDUN)[75]	A structured method for identifying privacy-specific threats at each stage of the data lifecycle.	Engineers use LINDDUN's seven threat categories to pinpoint and address privacy risks during the system design phase, before they become compliance failures.	Maps closely to DPDPA obligations on purpose limitation, data minimisation, and consent; supports DPIAs and PbD implementation.
NIST Cybersecurity Framework (CSF) 2.0[76]	An enterprise-wide approach to managing privacy risk across the full organisational lifecycle.	A voluntary, outcome-based framework that structures privacy risk management through five core functions: Identify-P (ID-P), Govern-P (GV-P), Control-P (CT-P), Communicate-P (CM-P), and Protect-P (PR-P), designed to work alongside broader cybersecurity risk management.	The five-function structure aligns directly with the DPDP framework's accountability, consent,[77] and data security obligations placed on Data Fiduciaries.
NIST Special Publication 800-30 Revision 1 (Guide for Conducting Risk Assessments)[78]	A step-by-step methodology for assessing information security and privacy risks.	Provides a structured process for identifying, analysing, and responding to risks across the system lifecycle, originally designed for federal systems but widely applicable to private organisations.	Supports DPIA processes and helps operationalise the "reasonable security safeguards" standard of the DPDP Act.[79]
NIST IR 8062 (An Introduction to Privacy Engineering and Risk Management in Federal Systems)[80]	Translates privacy policy requirements into concrete, measurable engineering objectives.	Introduces a Privacy Triad — Disassociability, Predictability, and Manageability — as practical design targets, treating privacy as an engineering property rather than a legal checkbox.	Directly supports DPDPA obligations on data minimisation, notices,[81] consent,[82] and individual rights by giving engineers a workable design framework.

Framework Name	Core Concept	Operational Implications	Relevance to the DPDP framework
ISO/IEC 27701:2019[83]	An international standard for building and maintaining a Privacy Information Management System.	Extends ISO 27001 and ISO 27002 to cover privacy-specific controls for both data controllers and processors, providing a certifiable compliance structure aligned with GDPR and OECD principles.	The closest existing international standard to a DPDP compliance management system is recommended as the baseline framework for India's forthcoming Privacy Certification Scheme.

Table: PTM Frameworks and Relevance to DPDP Framework

How PTM Enhances DPIA?

PTM provides a systematic, technical lens to feed into the DPIA, making it more effective and actionable:

- Identifies Relatability Risks: PTM maps how different datasets, when combined, could lead to re identification or profiling. DPIA then documents these risks explicitly, ensuring they are not overlooked.
- Contextual Risk Analysis: PTM considers the context of use, such as sharing data with downstream processors, AI model training, or cross border transfers. DPIA benefits by capturing risks beyond traditional security breaches, such as misuse or purpose drift.
- Granular Threat Scenarios: PTM generates detailed scenarios, such as linkage attacks, attribute disclosure, and insider misuse. DPIA can then evaluate likelihood and severity with greater precision.
- Designing Mitigation Measures: PTM points to technical controls like pseudonymisation, differential privacy, or synthetic data. DPIA records these as PbD measures, strengthening compliance evidence.
- Dynamic Risk Tracking: PTM is iterative; it evolves as systems, datasets, and processors change. DPIA becomes a living document, updated with PTM insights to reflect ongoing risk management.

ii. Data Security Posture Management

DSPM involves security practices and technologies that address the challenges posed by sensitive data spread across different environments.[84]

Key Characteristics

- Detection of misconfigurations, vulnerabilities, and unauthorised access.
- Provision of visibility into where sensitive data resides.
- Enforcing security policies and compliance baselines.

While DSPM is primarily security-focused, PTM is primarily focused on Privacy Risk Quantification for data in use and may be directly aligned with the scope of data protection and privacy obligation.

The table below maps both tools against DPDP compliance dimensions, not to establish one as superior, but to illustrate where each contributes and where they must work together. The gaps visible in DSPM's column are not indictments of DSPM as a tool; they illustrate the distinct and additive role privacy-specific governance must play alongside security controls.

Dimension	DPDP Provision Mapping	DSPM	PTM	Integrated Posture
Principles Covered	Grounds for Processing[85] Notices[86]	Enforces confidentiality; keeps unauthorised parties out	Checks disassociability and purpose alignment; evaluates consent context	Security controls and privacy purpose controls together satisfy the lawful basis obligation
Personal Data Discovery	Data Minimisation[87]	Discovers direct Personally Identifiable Information (PII) in configured environments	Discovers PII, quasi-identifiers, and statistical/ relatable data across flows	DSPM locates known PII repositories; PTM extends to relatable and derived data Both are needed for a complete data surface map

Dimension	DPDP Provision Mapping	DSPM	PTM	Integrated Posture
Identifiable and Relatable Data	Re-identification Risks[88] Consent[89] Certain Legitimate Uses[90]	Handles identifiable data; re-identification through combination is outside its designed scope	Models identifiability and relatability, detecting when non-sensitive datasets combine into a re-identification risk	DSPM secures the data at rest; PTM assesses whether authorised access could still produce a re-identification or purpose-breach risk
Consent Integration	Consent[91] Certain Legitimate Uses[92] Notice[93] Consent Manager[94]	Not designed for consent-state tracking; outside its security posture scope	Integrates consent state with PTM, DPIA, and RoPA; consent withdrawal becomes an enforceable access control	PTM fills the consent-enforcement gap; consent signals from PTM output can trigger DSPM's access controls
Privacy Risk Quantification	Duties of Data Fiduciary[95] Reasonable Security Safeguards[96] SDF Obligations[97]	Asserts security compliance posture; does not produce evidence of privacy risk metrics	Quantifies privacy risk by quality and quantity; produces demonstrable, evidence-based accountability artefacts	DSPM demonstrates security posture; PTM demonstrates privacy posture DPB enforcement will test both axes
Privacy Regulatory Recommendation	Notices[98] Reasonable Security Safeguards[99]	Identifies data location and misconfiguration Maps findings to security baselines, not privacy obligations	Maps discovered personal data to the specific DPDP obligation that applies and recommends the proportionate control	A complete compliance posture requires both: knowing where data is (DSPM) and knowing which obligation governs it (PTM)

Dimension	DPDP Provision Mapping	DSPM	PTM	Integrated Posture
DPIA and ROPA	DPIA Obligations for SDFs[100]	Not integrated with DPIA or ROPA workflows by design	Accelerates DPIA with quantified risk inputs; wired to RoPA for continuous compliance evidence	PTM's DPIA integration is additive: it does not replace the security evidence that DSPM feeds into the same assessment
Database and Flow-Level Risk	Reasonable Security Safeguards[101] Intimation of Personal Data Breach[102]	Assesses database-level risk; complementary DLP tools handle data-in-motion across flows	Covers both database and flow-level risk, and tests purpose limitation at the moment data moves	DSPM and DLP secure the channel; PTM assesses whether the flow itself is purpose-compliant (both are necessary under Section 8(5) of the DPDP Act)
Internal and Third-Party Impact	Data Processor obligations[103] Retention Limits[104]	The discovery scope is primarily internal environments; third-party processor flows require additional configuration	Applies to internal and third-party data sharing flows; covers Data Processor obligations	Together, they provide end-to-end visibility: DSPM inside the perimeter, PTM across the full data-sharing chain
Recommending PETs	Reasonable Security Safeguards[105]	Enforces encryption and access controls PET selection against privacy properties is outside its scope	Recommends the specific PET (pseudonymi-sation, differ-ential privacy, synthetic data) proportionate to disassociability, predictability, and manageabil-ity risk	DSPM enforces the PET once applied; PTM selects the right PET based on the privacy risk profile

Dimension	DPDP Provision Mapping	DSPM	PTM	Integrated Posture
Verifying PETs post-mitigation	SDF Periodic Audit Obligations[106]	Cannot verify that an applied PET achieved disassociability; verification is outside its designed function	Verifies disassociability, predictability, and manageability of the PET implementation, post-mitigation assurance	PTM closes the audit loop; DSPM's continuous monitoring confirms the security posture remains intact after the PET application
Assessment Frequency and Cost	SDF Periodic Audit Obligations[107]	Requires continuous discovery scanning; recurring cost scales with data environment size	One-time assessment per flow; quantifies risk proportionate to the specific processing activity	The two models are complementary in deployment: DSPM provides always-on posture visibility; PTM provides targeted, flow-level privacy assurance at design time

Table: Comparative Analysis of DSPM and PTM for DPDP Compliance

The table makes clear that security controls and privacy controls address structurally different risks and should be deployed as an integrated stack, not as alternatives. An organisation with strong DSPM but no PTM knows where its data is and who can access it but cannot confirm that authorised access is purpose-bound, consent-compliant, or DPDP-aligned. Conversely, a PTM-driven privacy programme without the security foundation that DSPM provides would lack the data visibility on which privacy controls depend.

Under the DPDP framework, both layers are required. The DPDP Act mandates reasonable security safeguards[108] (the domain of DSPM). The purpose limitation,[109] consent,[110] and data minimisation[111] obligations (the domain of PTM) operate on top of and in addition to those security safeguards, not instead of them. Organisations that treat these as a choice will find themselves compliant on one axis and exposed on the other. The DPDP Act, read alongside the Board's emerging enforcement posture, will eventually test both.

Data in Use Implications

Privacy risks evolve as personal data shifts from being at rest to active use via different processing methods, with more from authorised access misuse than from external threats. Traditional security access control models may fall short in addressing these issues, especially within complex, AI-driven data ecosystems governed by the DPDP Act.

i. Consent-Based Access Control (CBAC): Enforcing Purpose and Lawfulness at Runtime

CBAC addresses the structural limitations of Role-Based Access Control (RBAC)[112] by embedding privacy obligations directly into access control logic: rather than relying solely on organisational roles, it conditions access to personal data on the existence, scope, and

validity of a Data Principal's consent[113] or other lawful basis.[114] It scopes permissions to specific purposes, and updates access in real time when consent is withdrawn, modified, or expires, enabling granular controls such as allowing analytics while prohibiting profiling or AI model training.

CBAC translates legal requirements into enforceable technical controls at the Data in Use stage.

Privacy Enhancing Technologies

The data privacy sector has introduced distinct yet overlapping categories of tools: Privacy Management Technologies (PMTs) and PETs. To understand PETs, it is imperative to delineate the two technological categories to assess an organisation's approach to the foundations of data protection and privacy.

i. Privacy Management Technologies: The Compliance Layer

Privacy Management Technologies (PMTs) are governance and compliance-oriented tools designed to help organisations meet regulatory requirements and manage privacy risks. They focus on processes, oversight, and accountability. Some examples of PMTs include consent management (capturing and managing user consent for data processing), cookie management (ensuring compliance with tracking and cookie regulations), Data Principal Rights Management (enabling rights such as access, rectification, erasure, and portability),[115] incident management (handling data breaches and privacy incidents), data discovery (identifying and cataloguing personal data across systems), and PMT (assessing risks and vulnerabilities in data processing activities).

PMTs primarily focus on ensuring compliance, transparency, and accountability under laws such as the DPDP Act, the GDPR, the California Consumer Privacy Act (CCPA), and upcoming AI regulations globally.[116] They help organisations demonstrate that they are meeting obligations, but they don't necessarily unlock new business opportunities with data.

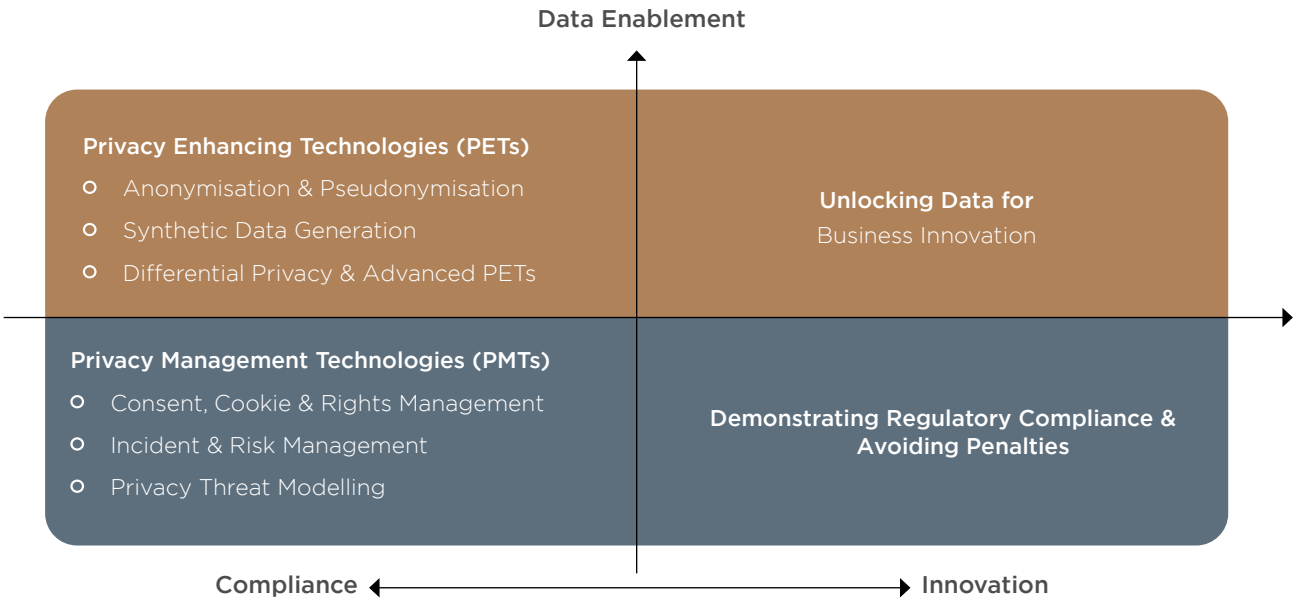


Figure: PETs and PMTs Framework for Data Enablement, Compliance, and Innovation

ii. Privacy Enhancing Technologies – Inculcating Privacy in System Architecture

PETs comprise a set of systems, processes, and technical techniques designed to enable the responsible use of data while minimising privacy risks.[117] As articulated by the OECD, PETs allow organisations to extract value from data without compromising confidentiality, thereby reconciling data utility with robust privacy protection.[118] Rather than relying solely on policy or procedural safeguards, PETs embed privacy controls directly into technical architectures, operationalising PbD at the system level.

By supporting secure data processing across collection, storage, use, and sharing, PETs help ensure end-to-end protection throughout the data lifecycle, even in complex or high-risk processing environments. They are particularly valuable where traditional access controls or anonymisation techniques are insufficient to address evolving threat models and regulatory expectations. The following table outlines some of the most commonly adopted PETs and their role in strengthening privacy governance while enabling data-driven innovation.

PET Typology	Key PETs	Explanation
Cryptographic Technologies	Homomorphic Encryption	Enables computation directly on encrypted data, so plain text is never exposed across lifecycle.
		Protects encrypted payloads as they move across networks; ciphertext remains opaque end-to-end.
		Preserves confidentiality during active use by allowing queries/aggregations over ciphertext.
	Zero-Knowledge Proof	Allows a prover to convince a verifier that a statement is true without revealing sensitive inputs.
	Secure Multi-Party Computation	Multiple parties jointly compute a function while keeping inputs secret from each other.
	Crypto-Shredding	Renders data irrecoverable by destroying or revoking encryption keys instead of wiping storage blocks.
Obfuscation Technologies	Pseudonymisation/ Anonymisation	Reduces identifiability by replacing direct identifiers and/or generalising attributes.
Obfuscation Technologies	K-Anonymity	Data is modified so that each person's information looks the same as at least k – 1 other people's information. This is done by hiding or broadening details (such as replacing exact ages with age ranges) so that no individual can be easily identified.
	Differential Privacy	Adds calibrated noise to queries/outputs to bound re-identification risk (privacy budget ε).

PET Typology	Key PETs	Explanation
Obfuscation Technologies	Dynamic Data Masking	System identifies personal entities like PII in unstructured data and images, dynamically mask them as per the required context. Traditional static masking provides basic protection but may not be of exemption grade as it is unaware of leakage through other attributes.
Statistical Technologies	Federated Learning	Trains a global model across decentralised datasets; only model updates (not raw data) are shared.
	Distributed Analytics	Pushes computation to where data resides (edge/on-prem) and aggregates safe summaries centrally.
	Synthetic Data Generation (SDG)	Creates statistically similar artificial datasets to reduce exposure of real PII.
Systems-Based and Account-ability Tech-nologies	Consent Mapping	Captures and enforces data subjects' consent, purposes, and restrictions across systems.
	Access Controls and Access Monitoring	Enforces least privilege access to stored datasets and monitors anomalies.
		Governs who can send/receive data; validates endpoints and protocols; audits transfers.
		Applies fine-grained controls to queries/jobs; tracks usage with purpose binding.
Systems-Based and Account-ability Tech-nologies	Data Dispersion	Reduces breach blast radius via sharding/erasure coding, as well as geo-distribution.
		Spreads traffic via CDNs/relay networks to limit correlation and single point exposure.

Table: PETs Typology[119]

iii. PETs Matrix: Translating into System Design

To enable understanding of PETs, their use cases, and their value propositions, we introduce this matrix:

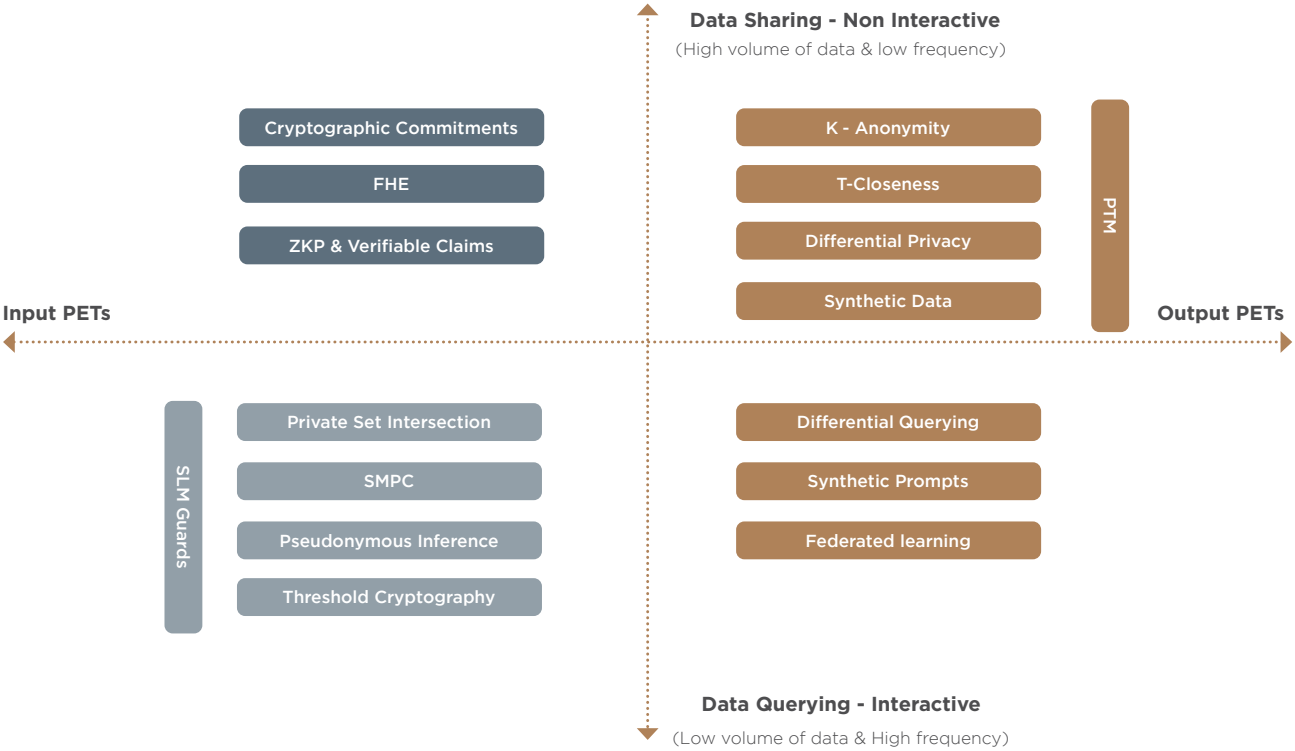


Figure: Classification of PETs

The vertical axis distinguishes non-interactive data sharing (high volume, low frequency; a one-time dataset handover) from interactive data querying (low volume, high frequency; live questions against data). The horizontal axis separates Input PETs (protection at data entry) from Output PETs (protection on released data). Input PETs secure data during processing, allowing collaboration without exposing raw inputs, addressing how to compute without seeing the data. Output PETs control what leaves the system, ensuring that no individuals can be reconstructed from the output, and focus on how to release data without leaking identities.

Key Terms to Consider

Privacy-preserved data sharing (non-interactive) involves bulk transfers, such as a bank providing a dataset to an analytics partner. The risk is total exposure of the entire dataset. In this case, data-altering Output PETs are predominant.[120]

Data querying (interactive) involves live API responses to multiple small queries, where cumulative risks arise as each answer leaks information. Runtime guards and query-budget PETs are crucial in this scenario.[121]

iii.a Output PETs — Non-Interactive Data Sharing (PTM Stage)

- **k-Anonymity**: Generalises quasi-identifiers so every record is indistinguishable from at least k–1 others. Prevents singling out an individual in a shared dataset. Weakness: Does not protect against attribute disclosure if a group shares a sensitive value.
- **t-Closeness**: Strengthens k-anonymity by requiring each equivalence group's sensitive-attribute distribution to stay within distance t of the overall distribution. Defends against attribute-disclosure and skew attacks that k-anonymity alone misses.
- **Differential Privacy**: Adds calibrated, mathematically bounded noise so the presence or absence of any one individual cannot be inferred from the output. Provides a formal, provable privacy guarantee, which is the strongest assurance for shared analytical outputs.
- **Synthetic Data**: Generates an artificial dataset that preserves statistical structure without containing any real records. Ideal for sharing, model training, and testing where utility lies in the distribution, not the individuals, which changes the data's DNA entirely.
- **PTM**: Not a PET itself but the governing layer for this quadrant — it quantifies privacy risk per data attribute and per flow, then prescribes which Output PET (and what parameter: the k, the t, the epsilon) is sufficient for that specific sharing scenario.

iii.b Output PETs — Interactive Data Querying

- **Differentially Private Querying**: Applies a differential-privacy budget across a live query stream, bounding cumulative leakage so an adversary cannot extract individuals by issuing many overlapping queries. The interactive counterpart to static differential privacy.
- **Synthetic Prompts**: Substitutes or sanitises real user inputs with synthetic equivalents before they reach a model, so sensitive content in prompts is never processed or logged in the clear during inference.
- **Federated Learning**: Trains a shared model across decentralised data sources; only model updates, never raw data, leave each site. Suited to interactive, distributed learning where data localisation, sensitivity, or sovereignty forbids centralisation.

iii.c Input PETs — Confidential Compute & Cryptographic (Data Sharing)

- **Confidential Compute (TEEs)**: Processes data inside hardware-isolated enclaves so it stays protected in use, shielded even from the host OS and operator. Allows sensitive financial or health data to be computed on without exposing it.
- **FHE (Fully Homomorphic Encryption)**: Performs arbitrary computation directly on encrypted data; the result decrypts correctly, but the processor never sees plaintext. Maximal input protection at significant compute cost.
- **Zero-Knowledge Proofs (ZKP) and Verifiable Claims**: ZKP lets one party prove a statement is true without revealing the underlying data. Verifiable claims extend this to credential-style assertions that prove eligibility or attributes without disclosing them.

iii.d Input PETs — SLM Guards (Interactive Inference)

- **Private Set Intersection (PSI)**: Let two parties find common elements (shared customers, overlapping records) without revealing the non-matching remainder of either set. Core to privacy-safe data matching and collaboration.
- **SMPC (Secure Multi-Party Computation)**: Multiple parties jointly compute a function over their combined inputs while each

input stays private to its owner. Collapses the trust requirement for collaborative analytics.

- **Pseudonymous Inference**: Strips or tokenises identity at query time so the model serves a request without ever processing who the subject is, thus the identity is decoupled from the inference.
- **Threshold Cryptography**: Splits a key or signing power across multiple parties so no single party can act alone; a threshold must cooperate. Distributes trust and removes single points of compromise.
- **Small Language Model (SLM) Guards**: The governing layer for this quadrant, SLMs act as runtime sentinels that screen prompts and responses, enforce policy, and invoke the input PETs above before sensitive data reaches the primary model.
- **Cryptographic Commitments**: Lets a party irrevocably "commit" to a value while keeping it hidden, revealing it later in a way that proves it wasn't changed. The integrity primitive underpinning ZKPs, verifiable claims, and auditable multi-party protocols.

The discussion establishes that risk-based privacy governance under the DPDP framework is a structured technical discipline rather than a simple compliance checklist. It involves three critical layers: data lifecycle mapping identifies personal data flows and associated obligations; PTM converts that awareness into quantified risk intelligence; and PETs implement embedded controls, such as homomorphic encryption and differential privacy. These layers are interdependent: PET selection without PTM is misguided, and PTM requires lifecycle mapping to be effective. Together, they embody the technical aspects of PbD that the DPDP framework enforces regarding purpose limitation, security, and data fiduciary accountability. Organisations that adopt this architecture before May 2027[122] will not only comply with regulations but also develop a proactive privacy posture that ensures genuine accountability rather than mere documentation-led compliance.

OPERATIONALISING PRIVACY BY DESIGN IN ENTERPRISES

PbD does not arrive in an organisation through a policy document. It arises from a decision made at the architecture stage, before a system is even built, that privacy obligations will govern how data moves, not merely how it is described. While literally, the DPDP Act does not use the phrase "Privacy by Design," but its structure encodes the expectation: lifecycle-oriented duties on Data Fiduciaries, enforceable rights for Data Principals, purpose limitation that binds processing at every stage, and security safeguard obligations that cannot be discharged through documentation alone. Organisations that read these obligations as a checklist will satisfy the letter of the law at a minimum-legal level. Organisations that read them as a design specification will build systems that are compliant by construction and demonstrably so when the Data Protection Board (DPB) begins enforcement. Further, as envisaged, stronger privacy compliance would also give them a competitive edge in the market, considering 'privacy' as a non-price factor.

ORGANISATIONS THAT READ THEM AS A DESIGN SPECIFICATION WILL BUILD SYSTEMS THAT ARE COMPLIANT BY CONSTRUCTION AND DEMONSTRABLY SO WHEN THE DATA PROTECTION BOARD BEGINS ENFORCEMENT.

With the implantability of PbD in mind, this chapter maps how the capabilities introduced in Chapters II and III, viz. consent and Data Principal rights,[123] PTM, DPIA, CBAC, and Privacy Enhancing Technologies, are operationalised as a connected governance lifecycle rather than parallel workstreams. The gap that most organisations will face is not a missing capability. It is a missing connection between existing capabilities.

Translating DPDP Obligations: Consent, Purpose Limitation, Minimisation, Retention, Erasure

The DPDP Act takes a lifecycle-oriented, accountability-driven approach to privacy governance. It requires Data Fiduciaries to uphold purpose limitation, data minimisation, accuracy, storage limitation, security safeguards, and timely erasure — and to honour these obligations not only within their own systems but across vendor ecosystems, digital supply chains, and organisational boundaries. The following

table maps each of the seven foundational PbD principles to its corresponding DPDP operational requirement and the technical intervention that gives it effect.

PbD Principle	DPDP Operational Requirement	Technical Intervention
Proactive, not Reactive; Preventative, not Remedial	Data Fiduciaries must implement ongoing security safeguards to prevent misuse, loss, or unauthorised access	PETs
Privacy as the Default Setting	Only necessary personal data may be collected with valid consent; it must be erased once the purpose is fulfilled unless retention is legally required	CBAC with PETs; Data Principal Rights Management
Privacy Embedded into Design	Organisations must build privacy into system design through technical safeguards such as encryption, obfuscation, and secure architectures	Input PETs; Output PETs
Full Functionality — Positive-Sum, not Zero-Sum	Personal data must be processed for lawful purposes, ensuring privacy without compromising usability or innovation	Data Principal Rights Management with CBAC and PETs
End-to-End Security — Lifecycle Protection	Personal data must be protected throughout its lifecycle, including accuracy, security safeguards,[125] and timely erasure	Access Controls and Monitoring; Data Dispersion; Crypto-Shredding; Confidential Computing
Visibility and Transparency	Clear notices in accessible language on collection, purpose, rights, and grievance mechanisms[126]	Consent Mapping; Data Audits; Management Interfaces; Access Controls and Monitoring
Respect for User Privacy — User-Centric Approach	Consent must be explicit and withdrawable; users must have access to grievance redressal and rights, including nomination and data access[127]	Consent Mapping; Management Interfaces; Access Controls; Synthetic Data Generation

Table: Mapping PbD Principles to DPDP Operational Requirements and Technical Interventions

An Integrated Architecture for Privacy by Design

As organisations mature their data protection programmes, a pattern emerges. The individual capabilities include a consent management system, a data discovery tool, a DPIA template, access controls, and PET implementations. Each is typically owned by a different function and built to a different timeline. Yet the outcomes that the DPDP Act requires are not reliably achieved. The failure does not lie within any individual's capability. It lies in what passes or fails to pass between them.

Consent is captured at collection and not consulted again. A Data Principal withdraws consent; the withdrawal is correctly recorded in the system of record, but the data has already been moved to downstream systems, where processing continues undisturbed. A DPIA is completed as a one-time template, detached from the risk quantification that PTM could have provided as structured input. PETs are selected and deployed without reference to the specific risk profile of the flow they are meant to address. Each system has performed as designed. The aggregate outcome is a privacy programme that is technically present and substantively incomplete.

The DPDP Act's obligations are designed as a lifecycle, not a list. Reading them in order makes the architecture visible.

I. Stage 1 — Consent and Data Principal Rights: Lawful Basis and Its Downstream Effect

The data lifecycle begins with a legal fact: every stage that follows depends on the basis on which processing is permitted, the purpose to which it is limited, and whether that basis remains valid. Consent[128] and Data Principal rights[129] are two aspects of this single fact: the permission and its limits, the grant and its withdrawal.

Under the DPDP Act, consent must be free, specific, informed, unconditional, and unambiguous, and its withdrawal must be as easy as its grant.[130] The practical implication is architectural. A consent withdrawal that is correctly recorded in the consent management system but not propagated to every downstream system where that data has moved does not satisfy the Act's intent. No individual system has failed; the failure is structural: the basis established at collection was never made available to the subsequent stages. The design requirement is that consent state travels with data, and that withdrawal triggers enforcement at every point of processing, not only at the point of record.

II. Stage 2 — Privacy Threat Modelling: Understanding Risk Before Selecting Controls

Before a safeguard can be chosen, the risk it is meant to address must be understood. PTM provides that understanding, not merely cataloguing where personal data exists, but quantifying the privacy risk that each data flow carries, accounting for relatability, re-identification potential, and purpose drift, not only direct identifiability.

A flow that appears unremarkable from a security standpoint may carry significant privacy risk. Attributes that identify no individual in isolation may, in combination or in context, re-identify a Data Principal. The DPDP Act's definition of personal data is broad precisely because the legislature understood this: the risk of re-identification is not confined to fields labelled as sensitive. PTM surfaces this risk per attribute and per flow and produces the structured, quantified output, a documented risk rationale, which the DPIA stage requires as input. A discovery exercise that locates personal data without quantifying its risk produces an inventory, and an inventory is not a reduction in exposure.

III. Stage 3 — Risk-Aware DPIA: The Decision That Connects Risk to Control

The DPIA sits at the centre of the PbD lifecycle because it is where risk understanding becomes a control decision. For SDFs under the DPDP Act, DPIA is a mandatory periodic obligation,

not a one-time exercise conducted at system launch and then shelved.[131] When the DPIA receives structured, quantified input from PTM, it functions as the DPDP framework intends: a determination of the appropriate safeguard for a specific risk in a specific flow, expressed as an actionable control and carried into the RoPA. When it does not, when it is completed as a template disconnected from the technical reality of the flow, it produces a document, not a decision.

At scale, the DPIA is not an occasional governance event but a continuous requirement that must keep pace with new processing activities, system changes, and evolving threat models. Approaches that cannot scale become constraints that delay legitimate data use. The design question for Significant Data Fiduciaries is how to preserve the rigour and human accountability the Act requires while enabling assessments to proceed at the velocity that modern data environments demand, a question that is substantially easier to answer when the DPIA receives structured inputs from PTM and feeds structured outputs into the access, and PET controls that follow.

IV. Stage 4 — CBAC and PETs: Enforcement at the Point of Use

Data governance is ultimately realised at the point where data is used. Consent-Based Access Control and Privacy Enhancing Technologies are the mechanisms through which the basis established at Stage 1, the risk understood at Stage 2, and the control determined at Stage 3 are enforced in the operating system.

Where a use case requires the actual record, such as servicing a Data Principal's account, responding to a rights request, or processing a transaction, CBAC binds access to the consented purpose, the authorised role, and the period for which the basis holds. Consent withdrawal does not generate a manual request; it revokes access in real time, across every system where that data is held. The governance decision taken at the DPIA stage is enforced at the moment of use, not after the fact.

PETs remove sensitive content from the processing path entirely where a use case does not require the actual record, such as analytics, model development, testing, collaboration with third parties, or regulatory reporting. The appropriate PET and its correct parameterisation are determined by the risk profile that PTM has quantified and the DPIA has evaluated. Differential privacy for shared analytical outputs. Federated learning for model training across decentralised datasets. Homomorphic encryption where computation on plaintext cannot be permitted. Synthetic data where the use case requires statistical fidelity, not individual accuracy. The technology is chosen because the risk demands it, not because it is available.

Why Integration Is Not Optional Under the DPDP Act

Each of the stages mentioned in the previous section are necessary. None is sufficient alone. The DPDP framework's obligations are not satisfied when consent is captured but not carried forward, when risk is understood but not used, when a DPIA is completed but disconnected from the control it should determine, or when a PET is deployed without the risk rationale that justifies its selection.

The DPB, when operational, will have access to audit powers, adjudication authority, and the ability to require organisations to demonstrate how their technical controls map to their stated lawful bases and processing purposes. Organisations that have built these stages as a connected lifecycle, where each stage informs and is honoured by the next, will be able to produce that demonstration. Organisations that have treated them as independent workstreams will find that the gaps between their capabilities are precisely where the enforcement questions land.

PbD under the DPDP framework is not an architectural preference. It is the difference between a compliance posture that holds under scrutiny and one that does not.

REGULATORY, SECTORAL, AND GLOBAL INSIGHTS

The DPDP framework has changed the perception of data protection in India from a fragmented approach to a more uniform regime. This chapter clarifies compliance with existing regulations and addresses challenges in navigating this landscape. By mapping the DPDP framework onto current norms and analysing foreign data protection regimes, it aims to provide actionable tasks for entities, helping regulators and policymakers manage overlaps effectively.

Sectoral Regulations and Privacy by Design

i. Banking, Financial Services and Insurance

Banking, Financial Services, and Insurance (BFSI) encompasses entities offering financial products or services. Key components include banking (commercial, investment, and non-banking financial companies), financial services (stock broking, mutual funds, payment gateways, and asset management), and insurance (life, general, and health).

Services	Regulatory Authority	Concerned Legislation
Banking and NBFCs	Reserve Bank of India (RBI)	RBI Act, 1934
Insurance companies	Insurance Regulatory and Development Authority of India (IRDAI)	IRDA Act, 1999
Other BFSI entities	Securities and Exchange Board of India (SEBI)	SEBI Act, 1992

Table: Regulatory Authorities and Legislation governing the Indian BFSI Sector

Digital disruption, including AI chatbots and real-time financial analytics, has enhanced capabilities and exposure. The main challenge is protecting consumer data while complying with overlapping regulations.

Banking and Financial Services

The RBI has long imposed data privacy and protection norms on regulated entities under its ambit, through advisories, circulars, and guidelines. There are also frameworks for using PETs to ensure the effective operation of online banking, among all practices, and the utmost care for a customer's personal data.

Legislations

- **The State Bank of India Act, 1955**: Allows disclosures only in legally sanctioned circumstances or when they serve the public interest, balancing privacy with national priorities.[132]
- **The Banking Companies (Acquisition and Transfer of Undertakings) Act, 1980**: Imposes obligations of fidelity and secrecy on public sector banks. Disclosures of customer information are permitted only when directed by legal authorities, ensuring compliance without breaching trust.[133]
- **The Public Financial Institutions (Obligation as to Fidelity and Secrecy) Act, 1983**: Mandates strict confidentiality standards for public financial institutions in handling sensitive customer data.[134]
- **The Credit Information Companies (Regulation) Act, 2005**: Obligates banks and financial institutions providing credit information to credit information companies to handle the same information with strict confidentiality.[135]
- **The Payment and Settlement Systems Act, 2007**: Prohibits system providers from disclosing information from participants unless required by law, with consent, or mandated by a court.[136]

Regulatory Guidelines

- **Guidelines on Cyber Security Framework in Banks, 2016**: Banks must protect customer information by encrypting data, restricting access to authorised personnel, and conducting regular audits.[137]
- **Know Your Customer (KYC) Direction, 2016**: Mandates the Implementation of data minimisation practices when collecting information for customer identity verification and the onboarding process.[138]
- **Master Direction – Information Technology Framework for the NBFC Sector, 2017**: Requires that NBFCs establish IT infrastructure with built-in data security and privacy controls.[139]
- **Storage of Payment System Data, 2018**: Mandates end-to-end data localisation of all payment data, with it being required to be stored exclusively within Indian territory.[140]
- **Master Direction – Reserve Bank of India (Digital Payment Security Controls) Directions, 2021**: Digital payment systems must incorporate security and privacy features from the outset.[141]
- **Reserve Bank of India (Outsourcing of Information Technology Services) Directions, 2023**: Regulated entities must ensure third-party IT vendors extend privacy obligations through contracts and oversight.[142]
- **Reserve Bank of India (Non-Banking Financial Companies – Managing Risks in Outsourcing) Directions, 2025**: NBFCs must ensure customer data confidentiality and privacy when outsourcing by practising due diligence, implementing contractual safeguards, and continuously monitoring service providers.[143]

Use case	DPDP provision	Capability	Problem with the traditional solution	PbD stack resolution
Call-centre access to customer records	Consent[144] Data Minimisation[145]	Consent CBAC	Agent sees the full customer record on login; access is role-based, not purpose-bound; consent is not checked at the time of access.	Access scoped to consented purpose; minimum fields exposed; all access logged; withdrawal effective immediately.
Marketing and cross-sell after consent withdrawal	Withdrawal of Consent[146] Reasonable Security Safeguards[147]	Consent CBAC	Withdrawal logged centrally, but live campaign data continues to be processed: a purpose breach, not a security breach.	Withdrawal propagates as a live signal; consent is checked at send time, not at list creation; processing halts across all platforms.
DPIA for a new product or data flow at the SDF scale	Additional Obligations of an SDF[148] Periodic Audit Requirements	Agentic DPIA	Static, manually approved templates: weeks-to-months per flow; unscalable across hundreds of applications; verdict disconnected from enforcement.	Automated, context-driven DPIA ingests PTM scores, outputs parameterised safeguards, and auto-populates RoPA; the DPO remains in the loop, reducing timelines from months to minutes.

Table: Practical Use Cases for PETs and PbD in the Banking and Finance Sector

Insurance

The IRDAI's regulatory policies prioritise policyholder protection, confidentiality, and accountability. The insurance sector collects substantial personal data, including health and financial details, to underwrite policies and customise premiums. Due to the sensitive nature of this data, stringent regulatory guidelines and the DPDP framework are essential for compliance with data protection principles.

Regulatory Guidelines

- **IRDAI (Maintenance of Insurance Records) Regulations, 2015**: Insurers must maintain electronic records of policies and claims as per regulations. These records, governed by insurer policies approved by their board, must ensure the privacy and security of policyholder and claim data. [149]
- **IRDAI (Protection of Policyholders' Interests) Regulations (2017, updated in 2024)**: Insurers must collect only necessary information for underwriting and claims.[150]
- **IRDAI Guidelines on Outsourcing, 2017**: Insurers must ensure that outsourced providers uphold similar data confidentiality and security standards, extending privacy obligations to third parties.[151]
- **IRDAI Sandbox Regulations, 2019**: Incorporates data protection requirements for experimental Fintech/Insurtech products, ensuring privacy controls are tested and embedded before full-scale deployment.[152]
- **IRDAI Information and Cyber Security Guidelines, 2023**: Insurers must implement end-to-end data security controls,

encryption, and access management frameworks to protect policyholder data across systems and third-party arrangements.[153]

Use case	DPDP provision	Capability	Problem with the traditional solution	PbD stack resolution
Underwriting on health and lifestyle data	Notice and Content of Notice[154] Retention Limitations[155]	Notice Consent PTM	Broad proposal-stage consent; medical data collected beyond the underwriting purpose; notice generic and not purpose-itemised.	Purpose-itemised, scoped notice and consent; PTM flags special-category attributes and enforces minimisation against the underwriting purpose.
Claims processing via TPAs and hospitals	Data Processor[156] Reasonable Security Safeguards[157]	CBAC PETs	Full record shared with TPA and hospitals; access role-based, not claim-bound; exposure exceeds claim needs.	Access scoped to claim and minimum fields; sensitive attributes masked/tokenised where not needed for adjudication.
AI in underwriting, claims triage and risk scoring	Rule s.13(3) (algorithmic processing); R.6(1)(b); IRDAI conduct norms	PTM PETs Agentic DPIA	Models cannot unlearn withdrawn consent; opaque decisions on sensitive attributes with weak audit and fairness evidence.	Privacy-preserving training on synthetic/ protected data; risk and fairness assessed pre-deployment; aligned to DPDP and IRDAI expectations.

Table: Practical Use Cases for PETs and PbD in the Insurance Sector

Securities and Capital Markets

The regulatory framework established by SEBI aims to enhance cybersecurity resilience, ensure market integrity, and protect investors. To achieve this, it is essential to incorporate PbD into the operations of platforms that handle personal data. This proactive approach helps prevent misuse, unauthorised access, and systemic risks arising from the large-scale handling of sensitive financial and personal data.

Legislations

- **The Depositories Act, 1996**: Mandates depositories to maintain a register and an index of beneficial owners, in the manner prescribed in the Companies Act, 1956, where records of personal details of members are maintained.[158]
- **The Prevention of Money Laundering Act, 2002, read with the Prevention of Money Laundering (Maintenance of Records) Rules, 2005**: Requires intermediaries to maintain transaction records and client identity for a period of five years.[159] Suspicious transactions are also to be reported to the FIU-IND.

Regulatory Guidelines

- **Securities and Exchange Board of India (Prohibition of Insider Trading) Regulations (2015, updated in 2025)**: Companies are mandated to maintain non-

negotiable, time-stamped, and audited records of all individuals who access Unpublished Price Sensitive Information.[160]

- **Security & Cyber Resilience Framework for Stock Brokers/Depository Participants (2018) and Mutual Funds/Asset Management Companies (2019)**: These frameworks incorporate privacy by design, requiring that sensitive data be protected through encryption, masking, and one-way cryptographic hashing, making personal and financial data unreadable and irreversible by default, both at rest and in transit.[161]
- **SEBI Circular on Cloud Services (2023)**: Regulated entities must ensure that their cloud infrastructure includes data security, sovereignty, and access controls to prevent privacy risks from third-party hosting.[162]
- **Master Circular on KYC Norms for the Securities Market (2023)**: Mandates data minimisation and purpose limitation principles by standardising the collection of only necessary client information for identity verification, while establishing centralised KYC records to avoid redundant and excessive data collection across multiple intermediaries.[163]
- **Policy for Sharing Data for Research/ Analysis (2024)**: Requires anonymisation or aggregation of data before it is disclosed for research purposes, ensuring individuals cannot be re-identified and that personal data is not exposed beyond its original collection purpose.[164]

Use case	DPDP provision	Capability	Problem with the traditional solution	PbD stack resolution
KYC collection at onboarding (broker / DP / RTA)	Notice and Content of Notice[165] Purpose Limitation Data Minimisation[166]	Notice Consent PTM	KYC collected under a broad notice and reused across functions; data gathered beyond the onboarding purpose.	Purpose-itemised, scoped notice and consent; PTM enforces minimisation against KYC purpose and flags reuse as requiring a fresh basis.
Investor data shared across the intermediary chain	Obligations relating to Data Processors[167] Reasonable Security Safeguards[168]	Consent CBAC PTM	Investor records flow to RTAs, DPs, and AMCs under contract; access is role-based, not purpose-bound; insider exposure surface is wide.	CBAC binds each intermediary to consented purpose and minimum fields; access is logged and revocable across the chain.
Market surveillance and trade-pattern analytics	Additional Obligations of an SDF[169] Certain Legitimate Uses[170] Periodic Audit Requirements	PTM PETs Agentic DPIA	Surveillance models on identifiable trade data drift from integrity monitoring to investor profiling without a reassessed legal basis.	DPIA reassesses the basis for the surveillance purpose; models are trained on synthetic/protected data; risk is quantified before the analytics pipeline runs.

Table: Practical Use Cases for PETs and PbD in the Securities and Capital Markets Sector

Healthcare

The healthcare sector, including the pharmaceutical industry, handles a significant amount of sensitive personal data, including health and biometric information. While Article 9 of the GDPR prohibits the processing of certain categories of data, such as health information and biometric data, the DPDP framework does not explicitly distinguish between sensitive personal data and other personal data. This agnostic nature provides a uniform standard for processing digital personal data across industries, while leaving certain regulatory gaps that may be addressed through sector-specific frameworks.

India also lacks a comprehensive data protection law for health data, similar to the US Health Insurance Portability and Accountability Act (HIPAA). A similar bill was proposed by the Ministry of Health and Family Welfare in India, the Digital Information Security in Healthcare Act (DISHA),[171] but it remains unrealized.

Regulatory Guidelines

- **Health Data Management Policy, 2020**: It establishes minimum privacy and data protection standards for the Ayushman Bharat Digital Mission ecosystem.[172] Health data cannot be shared with third parties without consent, and strict data minimisation applies.
- **Guidelines for Practice of Telemedicine in India, 2020 (updated in 2023)**: Mandates identity verification, consent, and documentation for virtual consultations; requires data privacy and professional conduct standards.[173]

Use case	DPDP provision	Capability	Problem with the traditional solution	PbD stack resolution
Clinical record access across hospital roles	Consent[174] and Purpose Limitation Data Minimisation Processing of Personal Data of Children[175]	Consent CBAC	Clinical staff see the full record regardless of care episode; access role-based, not episode-bound.	Access scoped to care episode and minimum clinical fields; logged, revocable; child data under stricter consent.
Consent for treatment vs research vs marketing	Notices,[176] Granular and Withdrawable Consent	Notices,[177] Consent	Single admission consent covers treatment, research and outreach; patients cannot withdraw for this purpose.	Granular, withdrawable consent per purpose; treatment, research and outreach each governed by a distinct legal basis.
Genomic and mental-health data processing	Consent Data Minimisation[178] Exemptions for Research: Additional Obligations of an SDF[179]	PTM PETs	Highest-sensitivity data processed identifiably; re-identification risk is acute even from small genomic or psychiatric datasets.	PTM flags the highest-risk attributes; data-altering and data-preserving PETs are applied to enable use without individual exposure.

Table: Practical Use Cases for PETs and PbD in the Healthcare Sector

Telecommunications, Media, and Technology (TMT)

As a result of the vast consumer data collected in this sector, the DPDP framework has become a strategic inflexion point for the TMT sector to redefine trust and lead in a now-privacy-conscious economy. The Telecom Regulatory Authority of India (TRAI) and the Department of Telecommunications (DoT) are key regulators in India's telecom sector. The DoT handles policy, licensing, and spectrum allocation, while TRAI focuses on consumer protection, tariffs, and network quality, advising the DoT. Together, they shape India's telecom landscape.

Regulatory Guidelines

- **TRAI Recommendations on Privacy, Security and Ownership of Data in Telecom Sector (2018)**: Explicitly recommends privacy by design as a regulatory principle for telecom operators, advocating for data minimisation, purpose limitation, and user consent frameworks built into network and service design.[180]
- **Telecom Commercial Communications Customer Preference Regulations (2018)**: Reflects consent-based data use by requiring explicit customer preferences before commercial communications, limiting the purpose of subscriber data use.[181]
- **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules (2021)**: Requires significant social media intermediaries and digital platforms to implement grievance redressal, data traceability, and privacy-protective measures as part of their platform architecture.[182]
- **Guidelines for Internet Service Providers (ISPs) under the Information Technology Act, 2000 / CERT-In Directions (2022)**: Mandates ISPs and intermediaries to maintain logs securely, report incidents, and implement controls around access to user data, embedding security into operational infrastructure.[183]
- **Telecommunications (Cyber Security) Rules, 2024 under the Telecommunications Act, 2023**: Requires telecom entities to implement security controls, report breaches, and protect traffic and user data from unauthorised interception or access by design.[184]

Use case	DPDP provision	Capability	Problem with the traditional solution	PbD stack resolution
CDR and location-data analytics/ monetisation	Additional Obligations of an SDF[185] Periodic Audit Requirements	PTM PETs	CDR/location datasets monetised in "anonymised" form are re-identifiable from a few mobility data points.	PTM quantifies re-identification risk; differential privacy or aggregation with mathematical guarantees applied before analytics or monetisation.
Commercial communi-cations and UCC consent	Withdrawal of Consent[186] Reasonable Security Safeguards[187]	Consent CBAC	Marketing consent siloed from data platforms; withdrawal not enforced downstream; UCC and DPDP compliance uncoordinated.	Consent state enforced as a live signal at send-time; DPDP withdrawal and TRAI UCC preferences unified in a single control.

Use case	DPDP provision	Capability	Problem with the traditional solution	PbD stack resolution
Licence-mandated retention vs erasure rights	Retention Limitations,[188] Rights of Data Principal[189] Exemptions for Research Archiving or Statistical Purposes[190] Telecom Act Conditions[191]	Consent PETs	Licence/security-mandated CDR and location retention conflicts with erasure requests; data remains re-identifiable beyond the relationship.	Retention bound to a statutory basis; data rendered unrelatable via PETs where the licence obligation is relied upon, removing the consent dependency.

Table: Practical Use Cases for PETs and PbD in the TMT Sector

Enforcing the DPDP Framework – The Data Protection Board and Its Role in Regulating Data Protection

The discussion on data privacy norms necessitates an authority for enforcing the law. The DPDP framework includes the DPB,[192] which is crucial for shaping regulatory practice, guiding compliance, and ensuring accountability in data protection governance. The DPB is the DPDP Act's primary enforcement body, operational since its Gazette Notification in November 2025.[193] Based in Delhi-NCR, the DPB, comprising four members, including a Chairperson, handles breach complaints, monitors fiduciary obligations, and adjudicates Data Principal rights.[194] Appeals lie to the Telecom Disputes Settlement and Appellate Tribunal.[195]

DPB as a means to operationalise PbD and PETs

The DPB can catalyse the mainstream adoption of PETs, serving not only as a compliance tool but also as a key part of the regulatory infrastructure for adhering to the DPDP framework and effectively implementing PbD principles, in the following manner:

- The DPB can require Data Fiduciaries to adopt PETs during personal data breach investigations or compliance directions, such as implementing data anonymisation before processing resumes.
- If a Data Fiduciary needs to prove consent or lawful processing of personal data, the DPB may also consider PETs that preserve privacy and support the Data Fiduciary's position.
- Like the Competition Commission of India (Determination of Monetary Penalty Guidelines), 2024,[196] where the implementation of a competition compliance program acts as a mitigating factor while determining the quantum of the penalty imposed on an entity, the DPB could treat the deployment of PETs by a Data Fiduciary as a mitigating factor.

- Dynamic Risk Tracking: PTM is iterative; it evolves as systems, datasets, and processors change. DPIA becomes a living document, updated with PTM insights to reflect ongoing risk management.

The role of the DPB is to execute the principle-based DPDP framework. The strategic use of PETs can make the technology an industry norm while also raising the country's data protection standards.

Global Insights into Privacy by Design and Privacy-Enhancing Technologies

i. European Union

Provisions regarding PbD and PETs

Article 25 of the GDPR requires Data Controllers to implement appropriate technical and organisational measures during processing, taking into account the state of the art and the risks to rights and freedoms.[197] Practices such as pseudonymisation and data minimisation are highlighted in Recital 78.[198] PbD is considered in DPIAs under Article 35 and during data breach investigations, with violations resulting in penalties of up to 4% of global turnover.[199]

The GDPR implicitly supports PETs through provisions on data protection by design and default[200], PETs such as encryption and pseudonymisation,[201] and the importance of proper design to avoid compliance gaps.[202] European regulators view PETs as crucial for PbD, risk mitigation in high-risk processing, and lawful data sharing. A report by the European Union Agency for Cybersecurity, titled "Privacy and Data Protection by Design – from Policy to Engineering", offers technical guidance that may serve as a benchmark for effective data protection measures.[203]

ii. United Kingdom

After the UK's exit from the EU, it now follows the UK GDPR, a regulation that closely resembles the EU GDPR. Instead of relying on statutory expansions, the UK has created guidance on data protection driven by regulatory bodies.

Provisions regarding PbD and PETs

The UK GDPR mandates organisations to embed PbD and privacy by default through appropriate technical and organisational measures to protect personal data.[204] To operationalise this compliance model, the framework enables organisations to consider the "state of the art" in privacy-preserving technologies when determining suitable measures.

The UK Information Commissioner's Office (ICO) guidelines on PETs allow the ICO to evaluate PbD through accountability documentation, DPIAs, and governance of technical controls in high-risk processing involving large-scale personal data collection and analysis, such as AI applications or cloud computing services.[205]

The ICO's Guidance, however, is under review after the Data (Use and Access) Act, 2025.[206]

iii. California

California does not expressly adopt the PbD terminology, but it embeds PbD-like obligations functionally within the CCPA (amended in 2020 by the California Privacy Rights Act) (CCPA and CPRA) and the implementing regulations of the California Privacy Protection Agency (CPPA).

Provisions regarding PbD and PETs

The CCPA requires businesses to adopt reasonable security procedures and practices, including administrative, technical, and physical safeguards.[207] The CPRA, effective in 2023, emphasises data minimisation, purpose limitation, and storage limitation as design-time constraints that lead to PbD outcomes,[208] requiring that the collection, use, retention, and sharing of personal information be reasonably necessary and proportionate to the stated purpose.[209] Section 1798.150 also allows consumers to bring a civil action if a business fails to secure their personal information and a breach occurs. The CPPA strengthens this framework by requiring formal risk assessments for high-risk processing[210] and cybersecurity audits for larger organisations[211], with phased implementation from 2026 to 2030.

The California Age-Appropriate Design Code Act, effective July 2024, goes further by mandating privacy protections by default for services likely to be accessed by minors, and requiring DPIAs prior to deploying features that process children's data: a hallmark of the PbD approach.[212]

Although PETs are not explicitly mentioned in statute, regulatory guidance under the CPPA cites encryption and automatic deletion as examples of safeguards businesses should consider,[213] and compliance analyses broadly treat PETs as practical mechanisms to satisfy the reasonable security standard, reduce breach exposure, and demonstrate accountability within risk assessment and audit frameworks.

iv. Singapore

Singapore incorporates PbD principles within the Personal Data Protection Act (PDPA) through regulatory guidance from the Personal Data Protection Commission (PDPC).

Provisions regarding PbD and PETs

The updated "Advisory Guidelines on the PDPA for Selected Topics"[214] (May 2024) includes a chapter on anonymisation, defining standards, assigning responsibilities, and requiring risk assessments to mitigate re-identification risks. Properly anonymised data may fall outside the PDPA's scope, encouraging the integration of privacy safeguards from the design stage.

The law mandates organisations to develop policies and practices to meet the obligations set out under the PDPA, as operationalised by the PDPC's guidance on documented processes and governance for anonymised data.[215] The PDPA also requires reasonable security safeguards to protect personal data from unauthorised actions,[216] while a limit on data retention to only what is necessary for business or legal purposes.[217]

Singapore promotes PET adoption through public-private collaborations, such as the PET Adoption Guide[218] and the PET Sandbox,[229] offering tools and pathways for technologies like differential privacy and federated learning. While not mandated, these technologies serve as practical controls to help organisations comply with PDPA accountability and security requirements, reduce risks, and ensure compliance during audits or regulatory engagements.

POLICY RECOMMENDATIONS AND IMPLEMENTATION PATHWAYS

The effectiveness of the DPDP Act depends on the enforcement of statutory obligations and the establishment of robust privacy governance across digital ecosystems. However, challenges persist in consistently applying data protection principles, despite laws and regulations governing them. Technologies such as cloud systems and AI require a transition from static compliance approaches to integrating data governance into system design, operational workflows, and technical controls throughout the data lifecycle.[220]

This chapter translates the white paper's findings into policy recommendations for two distinct audiences: industry stakeholders, and regulators and the government. The recommendations address institutional pathways, implementation mechanisms, and stakeholder roles to promote adoption across the public and private sectors and to support a transition from compliance-oriented approaches to continuous, risk-based privacy governance aligned with the DPDP Act and relevant international frameworks.

TECHNOLOGIES SUCH AS CLOUD SYSTEMS AND AI REQUIRE A TRANSITION FROM STATIC COMPLIANCE APPROACHES TO INTEGRATING DATA GOVERNANCE INTO SYSTEM DESIGN, OPERATIONAL WORKFLOWS, AND TECHNICAL CONTROLS THROUGHOUT THE DATA LIFECYCLE.

Governance and Accountability Frameworks

The absence of standardised data protection implementation guidance, despite organisations having clear ownership of information security and compliance functions, may result in inconsistent interpretations of data protection principles such as purpose limitation and data minimisation, leading to regulatory uncertainty and varying compliance maturity across sectors.[221]

To address these concerns, governance models, accountability frameworks, and operational procedures may be developed to integrate privacy considerations into organisational decision-making and system development processes.

i. Policy Recommendations: Strengthening Privacy Governance and Accountability

Industry Stakeholders

- Industry stakeholders may consider establishing cross-functional Privacy Governance Committees (PGCs) with a mandate to govern the full data lifecycle. Governance models proposed by the PGC could be structured around consent management, the rights of Data Principals,[222] PTMs, DPIAs, CBACs, and PETs.
    - Each pillar could have a designated convenor, documented integration points, and a direct reporting line to the DPB or its designated committee, consistent with Section 10 of the DPDP Act for SDFs.
    - Governance charters need to include explicit decision rights and defined authority over product and technology decisions to ensure cross-functional structures carry meaningful enforcement weight.
- Governance tiers should consider factors like data volume, nature, and the number of Data Principals. Micro, small, and medium enterprises (MSMEs) may use a simplified accountability model, such as a documented privacy register and a designated contact, as a temporary measure during the initial compliance period.

Sectoral Regulators and the Government

- The government may in consultation with the DPB, relevant sectoral regulators and industry experts from the concerned sector may consider issuing a document/ instrument that may give some guidance to industry on a proposed "DPDP Accountability and Privacy by Design Code of Practice" (Code of Practice) that would map DPDP obligations to specific governance and technical controls, and aligns with globally recognised governance frameworks such as the ISO standards and the NIST Privacy Framework.[223] This proposed Code of Practice may specify the nature of the obligations binding on Data Fiduciaries and SDFs, with the demarcation intended to prevent regulatory overreach or implementation fatigue.
- There could also be a development of open-source reference implementations, reusable privacy dashboard frameworks, and interoperable Data Fiduciary workflow architectures for DPIAs, RoPA, transfer impact assessments,[224] and privacy risk scoring[225] to reduce implementation barriers and improve consistency across organisations. These documents could be prepared collectively by regulators in consultation with industry stakeholders.

Technical and Operational Privacy Controls

Modern privacy risks arise primarily during the data-in-use stage, when personal data is processed and shared across systems.[226] Traditional perimeter-based security controls are often insufficient to address issues such as identifiability, linkability, and excessive data retention in artificial intelligence environments.[227] Accordingly, data governance should evolve to include technical controls that enforce purpose limitation, support data minimisation, enable consent-aware access, and provide real-time lifecycle governance, rather than relying solely on static policy documentation.[228]

i. Policy Recommendations: Operationalising Technical Privacy Controls

Industry Stakeholders

- Industry stakeholders may implement the usage of frameworks, including LINDDUN and the NIST Privacy Engineering principles (IR 8062), as a mandatory step before any new high-risk data flow enters production. This applies to organisations that process health, financial, location, or CDR data, as well as to those training AI/ML models on personal data. The output of such assessments may be documented and

made available to the DPB upon request or during an audit.

- Data Fiduciaries processing high-risk or large-scale personal data may be encouraged to maintain unified data inventories and lifecycle-based retention schedules aligned with the techno-legal framework recommended in the OPSA white paper, including automated deletion and anonymisation workflows for structured, unstructured, and AI-related datasets.[229]

Sectoral Regulators and the Government

- The government, sectoral regulators, and industry stakeholders may collaboratively publish a Baseline Technical Safeguards Profile (BTSP) mapping DPDP statutory obligations to minimum technical controls and defining anonymisation and pseudonymisation standards with technical specificity, including minimum k-anonymity parameters, differential privacy epsilon bounds for common use cases, and synthetic data fidelity requirements.
    - The parameters may be defined on a sector-specific basis, for example, appropriate epsilon values for aggregate public health statistics differ materially from those applicable to individual financial transaction data, with the development and revision of such sector-specific technicalities being looked into by a standing Technical Expert Group comprising privacy engineers, academic researchers, and sectoral specialists.
- The BTSP could also address the interaction between cross-border data transfer controls and security safeguards. Where the government restricts transfers under the DPDP Act, the BTSP, for instance, could specify how controls for cross-border data transfers, such as transfer impact assessments, pseudonymisation, and encryption-in-transit, could map to those restrictions. This would provide Data Fiduciaries with greater clarity in implementation and prevent regulatory arbitrage between data localisation requirements and cross-border processing arrangements.

Capacity Building and Institutional Enablement

The effectiveness of data governance frameworks depends not only on legal and technical design, but also on the institutional and human capabilities required to implement, operate, and maintain them. Many privacy failures arise from weak operational understanding and inconsistent organisational practices, rather than from the absence of formal controls. In addition, emerging governance approaches such as PbD, PTM, and data-in-use controls require specialised interdisciplinary expertise that remains underdeveloped within India's digital ecosystem.

i. Policy Recommendations: Building Privacy Governance Capacity

Industry Stakeholders

- Industry associations, academic institutions, and professional bodies may consider collaboratively developing practice-oriented privacy engineering programmes and sector-specific implementation registers that are focused on PbD implementation and PETs deployment. Such programmes would require defined competency standards against which a practitioner can be assessed, such as foundational privacy engineering literacy, PTM proficiency, DPIA capabilities, competence in implementing PETs, and AI and data lifecycle governance.
- To ensure near-term uptake, industry associations could promote a voluntary privacy capability self-assessment modelled on NIST CSF maturity tiers, allowing organisations to benchmark themselves and track progress annually.

Sectoral Regulators and the Government

- Academic and relevant professional accreditation bodies may consider integrating privacy engineering, application of the DPDP framework, AI ethics, PETs, and privacy risk management into the curricula of disciplines such as computer science, cybersecurity, law, data science, and public policy.
- The government could establish a Data Governance Coordination Committee, composed of the Chairperson of the DPB and senior representatives from sectoral regulators, with the aim of harmonising technical guidance on anonymisation standards, PTM methodologies, and PET usage; develop shared regulatory positions on AI privacy obligations, including model unlearning, algorithmic processing disclosure, and AI DPIA requirements; and coordinate enforcement approaches to prevent regulatory arbitrage.

CONCLUSION

The white paper indicates that effective privacy governance under the DPDP Act requires more than statutory obligations, consent formalities, or conventional cybersecurity measures. As India's digital economy expands through AI, Digital Public Infrastructure, and cross-sector data ecosystems, policy decisions will play an important role in shaping trust, innovation, and institutional resilience. Fragmented implementation and weak governance may contribute to systemic risks and compliance failures. In contrast, coherent and interoperable governance frameworks may help India emerge as a credible model for scalable data protection.

In this context, the global development of PbD and PETs indicates that data privacy and innovation are complementary rather than structurally opposed. The central implementation challenge is, therefore, not whether effective data governance is technically achievable, but whether governance frameworks, organisational capabilities, and institutional coordination mechanisms can evolve at a sufficient pace to support implementation at scale.

PbD should be understood not merely as a compliance obligation, but as an operational framework for the development of trustworthy digital systems. When embedded through governance structures, technical safeguards, lifecycle controls, and institutional accountability, privacy governance can function not as a constraint on digital transformation, but as an enabling condition for trust, resilience, and sustainable innovation.

This white paper is intended to provide a practical implementation pathway for operationalising privacy governance in India, grounded in technology, institutionally scalable, and aligned with the long-term objectives of a trusted digital economy.

REFERENCES

1. Alberts, D.S. & Papp, D.S. (1997), The Information Age: An Anthology on Its Impact and Consequences, CCRP Publication Series.
2. Kshetri, N. (2014), Big Data's impact on privacy, security and consumer welfare. Telecommunications Policy, 38(11), 1134-1145. https://doi.org/10.1016/j.telpol.2014.10.002.
3. Justice (Retd.) KS Puttaswamy v. Union of India, (2017) 10 SCC 1.
4. Supra at 2.
5. Katiyar, S. (2026, January 18). Privacy by Design vs Privacy by Checklist under the DPDP Act: What Healthcare Must Choose and Why, LinkedIn, http://linkedin.com/pulse/privacy-design-vs-checklist-under-dpdp-act-what-must-choose-katiyar-fxyaf/.
6. Digital Personal Data Protection Act, 2023, § 5 (India); see also Digital Personal Data Protection Rules, 2025, Rule 3.
7. Digital Personal Data Protection Act, 2023, § 6 (India).
8. Digital Personal Data Protection Act, 2023, § 2(i) (India).
9. Digital Personal Data Protection Act, 2023, § 8 (India).
10. Digital Personal Data Protection Act, 2023, § 8(5) (India); see also Digital Personal Data Protection Rules, 2025, Rule 6.
11. Digital Personal Data Protection Act, 2023, §§ 6(7)-6(9) (India); see also Digital Personal Data Protection Rules, 2025, Rule 4 (India).
12. Digital Personal Data Protection Act, 2023, §§ 11-15 (India).
13. Srinivasa, D.N. (2024), Privacy Enhancing Technologies: Global and Cross-Sectoral Regulatory Insights, Data Security Council of India. https://www.dsci.in/resource/content/privacy-enhancing-technologies.
14. Press Information Bureau. (2025, August 20). DPDP Act, 2023 Upholds Privacy While Preserving Transparency Under RTI. https://www.pib.gov.in/PressReleseDetailm.aspx?PRID=2158506&reg=3&lang=2.
15. Supra at 10.
16. International Organization for Standardization. (2023). ISO 31700:2023 — Consumer protection: Privacy by design for consumer goods and services – Part 1: High-level Requirements (ISO/IEC 3170-1:2023). https://www.iso.org/standard/84977.html.
17. International Organization for Standardization. (2018). ISO/IEC 20889:2018: Privacy enhancing data de-identification terminology and classification of techniques. ISO. https://www.iso.org/standard/69373.html.
18. Nieles, M., Dempsey, K., Pillitteri, V.Y. (2017), Introduction to Information Security (NIST Special Publication 800-12 Revision 1), National Institute of Standards and Technology, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf.
19. Jha, S. (2023). What About Accountability? Unfulfilled Expectations from the DPDP Act, 2023. Common Cause, 42(3), 20-23. https://www.commoncause.in/wotadmin/upload/July-Sept20-10-23-online.pdf.
20. Supra at 10.
21. Digital Personal Data Protection Act, 2023, § 8(7) (India); see also Digital Personal Data Protection Act, 2023, § 12(3) (India).
22. International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection — Information security management systems — Requirements (ISO/IEC 27001:2022). https://www.iso.org/standard/27001.
23. National Institute of Standards and Technology. (2024). The NIST cybersecurity framework (CSF) 2.0. U.S. Department of Commerce. https://www.nist.gov/cyberframework.
24. Organisation for Economic Co-operation and Development. (2013). The OECD privacy framework. OECD Publishing. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.
25. Supra at 22.

26. National Institute of Standards and Technology. (2020). NIST privacy framework: A tool for improving privacy through enterprise risk management, version 1.0. U.S. Department of Commerce. https://www.nist.gov/privacy-framework.
27. National Institute of Standards and Technology. (2017). An introduction to privacy engineering and risk management in federal systems (NIST Interagency Report 8062). U.S. Department of Commerce. https://doi.org/10.6028/NIST.IR.8062
28. Digital Personal Data Protection Act, 2023, § 2(t) (India).
29. Supra at 7.
30. A Data Protection Impact Assessment is a systematic risk assessment designed to help organisations identify, analyse, and minimise privacy risks associated with processing personal data.
31. Digital Personal Data Protection Act, § 10(2)(c) (India).
32. Digital Personal Data Protection Act, § 11(1)(a) (India).
33. Digital Personal Data Protection Act, § 2(j) (India).
34. Supra at 12.
35. Id.
36. Supra at 32.
37. Supra at 10.
38. Id.
39. Ali, W. & Arsalan, H. (2024). Ensuring Data Security and Privacy: Strategies for Targeted Data Discovery, Data Management Systems, and Private Data Access in Educational Settings, Department of Information Technology, University of GC Lahore, https://www.researchgate.net/publication/380664100_Ensuring_Data_Security_and_Privacy_Strategies_for_Targeted_Data_Discovery_Data_Management_Systems_and_Private_Data_Access_in_Educational_Settings.
40. Supra at 26.
41. Supra at 23.
42. Id.
43. Supra at 13.
44. Digital Personal Data Protection Act, 2023, §§ 5-7 (India).
45. Supra at 12.
46. National Institute of Standards and Technology. (n.d.). Personally identifiable information. NIST Computer Security Resource Center Glossary, https://csrc.nist.gov/glossary/term/personally_identifiable_information.
47. Supra at 28.
48. Supra at 8.
49. Digital Personal Data Protection Act, 2023, § 11 (India).
50. Supra at 30.
51. Supra at 11.
52. Digital Personal Data Protection Act, 2023, §§ 8(4), 8(5), 17(2)(b); see also Digital Personal Data Protection Rules, 2025, Rules 6 and 12.
53. Id.
54. Supra at 52.
55. Senarath, A. & Arachchilage, N.A.G. (2019). A data minimization model for embedding privacy into software systems, Computers & Security, 87, https://www.sciencedirect.com/science/article/abs/pii/S0167404818309106.
56. Karthik, A., Taneja, A., Srinivasan, S. & Sinha, V. (2026). Handbook on Data Protection and Privacy for Developers of Artificial Intelligence (AI) in India, Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH, https://www.nasscom.in/ai/pdf/handbook_for_ai_developers.pdf.
57. The World Bank. (2024). Navigating Data Governance: A Guiding Tool for Regulators, https://digitalregulation.org/navigating-data-governance-a-guiding-tool-for-regulators/.
58. Supra at 2.
59. Tibebu, H. (2024), Framework for Data Protection, Security, and Privacy in AI Applications, National Institute

of Standards and Technology, https://www.nist.gov/system/files/documents/2024/02/16/ID048%20-%20 2024-02-03%2C%20Loughborough%20University%2C%20Comments%20on%20AI%20EO%20RFI.pdf.

60. Jain, A., Thakur, K. & Agarwal, T. (2026). Strengthening AI Governance through Techno-Legal Framework, Office of the Principal Scientific Advisor to the Government of India, https://psa.gov.in/CMS/web/sites/default/files/publication/AI-WP_TechnoLegal.pdf.
61. Berkowitz, J., Mangold, M., & Sharon, S., (2017). Data Flow Maps – Increasing Data Processing Transparency and Privacy Compliance in the Enterprise, Washington and Lee Law Review Online, 73(2), 802-828, https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=1076&context=wlulr-online; see also Ofner, M., Straub, K., Otto, B., & Oesterle, H. (2013). Management of the Master Data Lifecycle: A Framework for Analysis, Journal of Enterprise Information Management, 26(4), 472-491, DOI:10.1108/JEIM-05-2013-0026.
62. Id.
63. Supra at 6.
64. Supra at 7.
65. Supra at 21.
66. Id.
67. Supra at 10.
68. Supra at 12.
69. Supra at 7.
70. Supra at 7.
71. Supra at 12.
72. Montauban, N (2025, September 02). What is privacy threat modelling? A conversation with two experts, Codific, https://codific.com/privacy-threat-modeling/?utm_source=chatgpt.com#Why_is_it_important.
73. Liu, S (2025). Modeling interdependent privacy threats, International Journal of Information Security, 24(224), https://doi.org/10.1007/s10207-025-01135-8.
74. Id.
75. Robles-González, A., Parra-Arnau, J., & Forné, J. (2020). A LINDDUN-Based framework for privacy threat analysis on identification and authentication processes, Computers & Security, 94, https://doi.org/10.1016/j.cose.2020.101755.
76. Supra at 16.
77. Supra at 7.
78. National Institute of Standards and Technology. (2012). Guide for conducting risk assessments (NIST Special Publication 800-30 Rev. 1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-30r1.
79. Supra at 8.
80. Supra at 27.
81. Supra at 6.
82. Supra at 7.
83. Supra at 15.
84. What is data security posture management (DSPM)? (n.d.). IBM, http://ibm.com/think/topics/data-security-posture-management.
85. Digital Personal Data Protection Act, 2023, § 7 (India).
86. Supra at 6.
87. Digital Personal Data Protection Act, 2023, §§ 6(1)(b) and 8(3) (India).
88. Supra at 28.
89. Supra at 7.
90. Digital Personal Data Protection Act, 2023, § 7 (India).
91. Supra at 7.
92. Supra at 90.
93. Supra at 6.
94. Supra at 11.
95. Supra at 9.

96. Supra at 10.
97. Supra at 31.
98. Supra at 6.
99. Supra at 10.
100. Supra at 31.
101. Supra at 10.
102. Digital Personal Data Protection Act, 2023, § 8(6) (India).
103. Supra at 8.
104. Supra at 21.
105. Supra at 10.
106. Supra at 31.
107. Supra at 31.
108. Supra at 10.
109. Supra at 87.
110. Supra at 7.
111. Digital Personal Data Protection Act, 2023, § 8(3) (India).
112. RBAC stands for Role-Based Access Control and is a security method that restricts system and data access to authorised users based on their specific job responsibilities or roles within an organisation.
113. Supra at 7.
114. Supra at 90.
115. Supra at 12.
116. Anam, J. (2025). Global Legal Responses to Deepfakes: A Regulatory Primer. Indian Governance and Policy Project. https://www.igap.in/global-legal-responses-to-deepfakes-a-regulatory-primer/.
117. Centre for Information Policy Leadership. (2023, December 12). Privacy-Enhancing and Privacy-Preserving Technologies: Understanding the Role of PETs and PPTs in the Digital Age, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-understanding-pets-and-ppts-dec2023.pdf.
118. Organisation for Economic Co-operation and Development. (2023). Emerging privacy-enhancing technologies: Current regulatory and policy approaches, https://www.oecd.org/en/publications/emerging-privacy-enhancing-technologies_bf121be4-en.html.
119. Supra at 26.
120. Afsharinia, B., Gurtoo, A., Dutta, J., and Malieckal, M. (2025). Privacy-Preserving Data Sharing: A Comprehensive Literature Review. Data for Public Good. https://dataforpublicgood.org.in/papers/data-policy/privacy-preserving-data-sharing-a-comprehensive-literature-review/.
121. Ritchie, M. (2025, January 31). What is Data Querying, Definite, https://www.definite.app/blog/what-is-data-querying.
122. Ministry of Electronics and Information Technology. (2025, November 13). Digital Personal Data Protection Rules, 2025 (Gazette Notification No. G.S.R. 846(E)). Government of India.
123. Supra at 12.
124. Supra at 10.
125. Id.
126. Supra at 6.
127. Supra at 12.
128. Supra at 7.
129. Supra at 12.
130. Supra at 7.
131. Supra at 31.
132. The State Bank of India Act, 1955, § 44 (India).
133. The Banking Companies (Acquisition and Transfer of Undertakings) Act, 1980, §13 (India).
134. The Public Financial Institutions (Obligation as to Fidelity and Secrecy) Act, 1983, § 3 (India).

135. The Credit Information Companies (Regulation) Act, 2005, § 29 (India).
136. The Payment and Settlement Systems Act, 2007, § 22 (India)
137. Reserve Bank of India. (2016, June 2). Cyber security framework in banks (Circular No. RBI/2015-16/418, DBS. CO/CSITE/BC.11/33.01.001/2015-16). https://www.rbi.org.in/commonperson/english/scripts/Notification.aspx?Id=1721
138. Reserve Bank of India. (2016, February 25). Master Direction – Know Your Customer (KYC) Direction, 2016 (Master Direction No. DBR.AML.BC.No.81/14.01.001/2015-16; updated August 14, 2025). https://www.rbi.org.in/CommonPerson/english/scripts/notification.aspx?id=2607
139. Reserve Bank of India. (2017, June 8). Master Direction – Information Technology framework for the NBFC sector (Master Direction No. DNBS.PPD.No.04/66.15.001/2016-17). https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10999
140. Reserve Bank of India. (2019, June 26). Frequently asked questions: Storage of payment system data. https://www.rbi.org.in/commonman/english/scripts/FAQs.aspx?Id=2995
141. Reserve Bank of India. (2021, February 18). Master Direction – Reserve Bank of India (Digital Payment Security Controls) Directions, 2021 (Circular No. RBI/2020-21/74, DoS.CO.CSITE.SEC.No.1852/31.01.015/2020-21). https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12032
142. Reserve Bank of India. (2023, November 7). Master Direction – Reserve Bank of India (Information Technology Governance, Risk, Controls and Assurance Practices) Directions, 2023 (Circular No. RBI/2023-24/102, DoS. CO.CSITEG/SEC.1/31.01.015/2023-24). https://www.rbi.org.in/scripts/BS_ViewMasDirections.aspx?id=12486
143. Reserve Bank of India. (2025, November 28). Master Direction – Reserve Bank of India (Non-Banking Financial Companies – Managing Risks in Outsourcing) Directions, 2025 (Circular No. RBI/DOR/2025-26/363, DOR.ORG.REC.No.282/21-04-158/2025-26). https://rbi.org.in/scripts/BS_ViewMasDirections.aspx?id=12941
144. Supra at 7.
145. Supra at 20.
146. Digital Personal Data Protection Act, 2023, §§ 6(4) to 6(6), (India).
147. Supra at 10.
148. Supra at 9.
149. Government of India. (2015, August 20). The Gazette of India: Extraordinary, Part III—Section 4: Insurance Regulatory and Development Authority of India (Maintenance of Insurance Records) Regulations, 2015 (No. 282). Insurance Regulatory and Development Authority of India.
150. Insurance Regulatory and Development Authority of India. (2024, September 5). Master circular on protection of policyholders' interests, 2024 (Ref. No. IRDAI/PP&GR/CIR/MISC/117/9/2024). https://irdai.gov.in/document-detail?documentId=5625747
151. Insurance Regulatory and Development Authority of India. (2017, April 20). IRDAI (Outsourcing of activities by Indian insurers) regulations, 2017. https://irdai.gov.in/document-detail?documentId=604638
152. Insurance Regulatory and Development Authority of India. (2019, July 26). IRDAI (Regulatory sandbox) regulations, 2019 (Notification No. IRDA/Reg/11/162/2019). Ministry of Finance, Government of India. https://financialservices.gov.in/beta/sites/default/files/2024-11/IRDAI%20%28Regulatory%20Sandbox%29%20Regulations%2C%202019.pdf
153. Insurance Regulatory and Development Authority of India. (2023). IRDAI information and cyber security guidelines, 2023. https://irdai.gov.in/document-detail?documentId=3314780
154. Supra at 6.
155. Supra at 21.
156. Supra at 8.
157. Supra at 10.
158. The Depositories Act, 1996, § 11 (India).
159. The Prevention of Money Laundering Act, 2002, §12(3) (India).
160. Securities and Exchange Board of India. (2015, March 12). Securities and Exchange Board of India (Prohibition of Insider Trading) Regulations, 2015 (last amended March 12, 2025). https://www.sebi.gov.in/legal/regulations/mar-2025/securities-and-exchange-board-of-india-prohibition-of-insider-trading-regulations-2015-last-amended-on-march-12-2025-_92672.html
161. Securities and Exchange Board of India. (2018, December 3). Cyber security & cyber resilience framework for

stock brokers / depository participants (Circular No. SEBI/HO/MIRSD/CIR/PB/2018/147). https://www.sebi.gov.in/legal/circulars/dec-2018/cyber-security-and-cyber-resilience-framework-for-stock-brokers-depository-participants_41215.html; see also Securities and Exchange Board of India. (2019, April 11). Technology committee for mutual funds / asset management companies (AMCs) (Circular No. SEBI/HO/IMD/DF2/CIR/P/2019/058). https://www.sebi.gov.in/legal/circulars/apr-2019/technology-committee-for-mutual-funds-asset-management-companies-amcs-_42692.html

162. Securities and Exchange Board of India. (2023, March 6). Framework for adoption of cloud services by SEBI regulated entities (REs) (Circular No. SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033). https://www.sebi.gov.in/legal/circulars/mar-2023/framework-for-adoption-of-cloud-services-by-sebi-regulated-entities-res-_68740.html
163. Securities and Exchange Board of India. (2023, October 12). Master circular on know your client (KYC) norms for the securities market. https://www.sebi.gov.in/legal/master-circulars/oct-2023/master-circular-on-know-your-client-kyc-norms-for-the-securities-market_77945.html
164. Securities and Exchange Board of India. (2024, December 20). Policy for sharing data for the purpose of research / analysis (Circular No. SEBI/HO/DEPA-II/DEPA-II_SRG/P/CIR/2024/178). https://www.sebi.gov.in/legal/circulars/dec-2024/policy-for-sharing-data-for-the-purpose-of-research-analysis_90088.html
165. Supra at 6.
166. Supra at 20.
167. Digital Personal Data Protection Act, 2023, §§ 2(k) and 8(2) (India).
168. Supra at 10.
169. Supra at 49.
170. Supra at 90.
171. Ministry of Health and Family Welfare, Government of India. (2017). Draft Digital Information Security in Healthcare Act (DISHA).
172. Ayushman Bharat Digital Mission. (n.d.). National Digital Health Mission: Health data management policy. Ministry of Health and Family Welfare, Government of India. https://abdm.gov.in/strapicms/uploads/health_management_policy_bac9429a79.pdf
173. Board of Governors in Supersession of the Medical Council of India. (2020, March 25). Telemedicine practice guidelines. Ministry of Health and Family Welfare, Government of India. https://esanjeevani.mohfw.gov.in/assets/guidelines/Telemedicine_Practice_Guidelines.pdf
174. Supra at 7.
175. Digital Personal Data Protection Act, 2023, § 9 (India); see also Digital Personal Data Protection Rules, 2025, Rule 10.
176. Supra at 6.
177. Supra at 6.
178. Supra at 20.
179. Supra at 49.
180. Indian Computer Emergency Response Team. (2022, April 28). Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for safe & trusted internet (No. 20(3)/2022-CERT-In). Ministry of Electronics and Information Technology, Government of India. https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf
181. Telecom Regulatory Authority of India. (2018, July 19). Telecom Commercial Communications Customer Preference Regulations, 2018. https://thc.nic.in/Central%20Governmental%20Regulations/Telecom%20Commercial%20Communications%20Customers%20Preference%20Regulation,%202018..pdf
182. Ministry of Communications, Department of Telecommunications. (2024, August 28). Telecommunications (Telecommunication Cyber Security) Rules, 2024 (G.S.R. 520(E)). Government of India. https://dpo-india.com/Resources/privacy_laws_in_India/Telecommunications-Telecom-Cyber-Security-Rules-2024(English-Version).pdf
183. Ministry of Electronics and Information Technology. (2021, February 25). The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (updated February 10, 2026). Government of India. https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf

184. Telecom Regulatory Authority of India. (2018, July 16). Recommendations on privacy, security and ownership of the data in the telecom sector. https://www.trai.gov.in/sites/default/files/2024-09/RecommendationDataPrivacy16072018.pdf
185. Supra at 49.
186. Digital Personal Data Protection Act, 2023, §§ 6(4) to 6(6), (India).
187. Supra at 10.
188. Supra at 21
189. Supra at 12
190. Supra at 28.
191. Telecommunications Act, 2023, § 20 (India).
192. Ministry of Electronics and Information Technology. (2025, November 13). Digital Personal Data Protection Rules, 2025 (Gazette Notification No. G.S.R. 846(E)). Government of India. https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf
193. Ministry of Electronics and Information Technology. (2025, November 17). DPDP Rules, 2025 notified: A citizen-centric framework for privacy protection and responsible data use (Release ID: 2190655). Press Information Bureau, Government of India. https://www.pib.gov.in/PressReleaseDetail.aspx?PRID=2190655&reg=6&lang=1
194. Storyboard18. (2025, November 14). Breaking: Data Protection Board to have a chairperson and four members, headquarters set in Delhi. https://www.storyboard18.com/digital/breaking-data-protection-board-to-have-a-chairperson-and-four-members-headquarters-set-in-delhi-84203.htm
195. Telecom Disputes Settlement & Appellate Tribunal. (2026, January 15). Vacancy circular (No. 3/7/2013Vol-V/Admn. TDSAT). Government of India. https://delhihighcourt.nic.in/files/2026-01/recuritment/vacancy_circular_tdsat_15.01.2026.pdf
196. Competition Commission of India. (2024, March 6). The Competition Commission of India (Determination of Monetary Penalty) Guidelines, 2024 (Notification No. B-14011/1/2024-ATD-II). Government of India. https://www.cci.gov.in/legal-framwork/regulations/92/0
197. European Union. (2016). Article 25: Data protection by design and by default. In Regulation (EU) 2016/679 (General Data Protection Regulation). https://gdpr-info.eu/art-25-gdpr/
198. European Union. (2016). Recital 78. In Regulation (EU) 2016/679 (General Data Protection Regulation). https://gdpr-info.eu/recitals/no-78/ (gdpr-info.eu)
199. European Union. (2016). Article 35: Data protection impact assessment. In Regulation (EU) 2016/679 (General Data Protection Regulation). https://gdpr-info.eu/art-35-gdpr/ (gdpr-info.eu)
200. Supra at 171.
201. European Union. (2016). Article 32: Security of processing. In Regulation (EU) 2016/679 (General Data Protection Regulation). https://gdpr-info.eu/art-32-gdpr/.
202. Supra at 173.
203. European Union Agency for Network and Information Security. (2015). Privacy and data protection by design: From policy to engineering. ENISA. https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design
204. United Kingdom. (2021). Article 25: Data protection by design and by default. In UK General Data Protection Regulation (UK GDPR). https://www.legislation.gov.uk/eur/2016/679/article/25 (legislation.gov.uk)
205. Information Commissioner's Office. (2023). Privacy-enhancing technologies (PETs). https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/
206. Data (Use and Access) Act, 2025 (UK).
207. California Civil Code § 1798.100(e). (2025). California Consumer Privacy Act of 2018. https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.100
208. California Civil Code § 1798.100(a)–(c). (2025). California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act. https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.100&lawCode=CIV
209. California Civil Code § 1798.100(c). (2025). California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act. https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.100&lawCode=CIV

210. California Code of Regulations, tit. 11, §§ 7150–7158. (2025). Cybersecurity audits, risk assessments, automated decision-making technology, and insurance companies. https://cppa.ca.gov/regulations/
211. California Code of Regulations, tit. 11, §§ 7120–7124. (2025). General rules governing consumer requests and business practices. https://cppa.ca.gov/regulations/
212. California Civil Code §§ 1798.99.30(a)–(b). (2025). California Age-Appropriate Design Code Act. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.48
213. California Privacy Protection Agency. (2025). § 7002(d)(3). In California Consumer Privacy Act regulations. https://cppa.ca.gov/regulations/
214. Personal Data Protection Commission Singapore. (2024). Advisory guidelines on the Personal Data Protection Act for selected topics (Rev. May 2024). https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/ag-on-selected-topics/advisory-guidelines-on-the-pdpa-for-selected-topics-%28revised-may-2024%29.pdf
215. Singapore. (2020). §11. In Personal Data Protection Act 2012. https://sso.agc.gov.sg/Act/PDPA2012
216. Singapore. (2020). §24. In Personal Data Protection Act 2012. https://sso.agc.gov.sg/Act/PDPA2012
217. Singapore. (2020). §25. In Personal Data Protection Act 2012. https://sso.agc.gov.sg/Act/PDPA2012
218. Infocomm Media Development Authority. (2025). Privacy Enhancing Technologies (PETs) adoption guide. https://www.imda.gov.sg/activities/activities-catalogue/pets-adoption-guide
219. Personal Data Protection Commission Singapore. (2022, July 20). Launch of Privacy Enhancing Technologies Sandbox. https://www.pdpc.gov.sg/news-and-events/announcements/2022/07/launch-of-privacy-enhancing-technologies-sandbox
220. Colombo, M. & Flynn, G. (2025). Data governance in the age of AI, KPMG, https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2025/data-governance-age-ai.pdf.
221. Lonzetta, AM & Hayajneh, T. (2020). Challenges of Complying with Data Protection and Privacy Regulations. EAI Endorsed Transactions on Scalable Information Systems, 10.4108/eai.26-5-2020.166352.
222. Supra at 12.
223. Supra at 25.
224. GDPR Register. (n.d.). Data transfer impact assessments. GDPR Register. https://www.gdprregister.eu/articles/data-transfer-impact-assessments/.
225. National Institute of Standards and Technology. (2021). Privacy Risk Assessment Methodology (PRAM). NIST. https://pages.nist.gov/nccoe-mdl-project-static-website/pram.html
226. Supra at 118.
227. Billiris, G., Gill, A. & Bandara, M. (2025). Privacy in the Age of AI: A Taxonomy of Data Risks. Australasian Conference on Information Systems. https://arxiv.org/pdf/2510.02357.
228. Id.
229. Supra at 61.

Authors

Anahida Bhardwaj, Associate – Privacy & Policy, DSCI

Deepa Ojha, Manager - Privacy & Policy, DSCI

Abilash Soundararajan, Founder & CEO, PrivaSapien

Alen Pious, Privacy Engineering Consultant, PrivaSapien

Contributor

Mridushi Bose, Senior Associate- Marketing & Communications, DSCI

PROMOTING DATA PROTECTION

The Data Security Council of India (DSCI), a Nasscom initiative, is a premier think tank on data protection, cyber security and emerging tech in India. DSCI engages with governments, regulators, industry, and academia to build a secure and trusted cyberspace through policy advocacy, thought leadership, and capacity-building initiatives.

PrivaSapien

Evolution for the Privacy & AI Era

PrivaSapien is a deep-tech pioneer dedicated to driving the "Evolution for the Privacy & AI Era." We empower global enterprises with cutting-edge privacy management and Privacy-Enhancing Technologies across the entire Data and AI lifecycle. Backed by a team of privacy visionaries holding over 30 patents, we embed "Privacy by Design" into the digital fabric of businesses through provable, verifiable, and ethical data safeguards. By championing Human-First AI and utilizing the PASSFERS framework, PrivaSapien solves mission-critical challenges—transforming privacy bottlenecks into scalable breakthroughs that allow organisations to unlock data value and innovate securely.

DATA SECURITY COUNCIL OF INDIA

Nasscom Campus, Fourth Floor, Plot. No. 7-10, Sector 126, Noida, UP - 201303

+91-120-4990253 | info@dsci.in | www.dsci.in

DSCI_Connect dsci.connect dsci.connect data-security-council-of-india dscivideo