

Data Protection by Design under the Digital Personal Data Protection Framework: Emerging Obligations and Regulatory Challenges in India

AUTHOR- DEEKSHA PANDEY

DESIGNATION- RESEARCH SCHOLAR (Ph.D in Law, Pursuing)

AFFILIATION- INSTITUTE OF LEGAL STUDIES, SHRI RAM SWAROOP MEMORIAL UNIVERSITY, LUCKNOW – DEVA ROAD, BARABANKI, 225003

EMAIL ID- pandeydeeksha71@gmail.com

Abstract

The rapid expansion of India's digital economy has intensified the collection, processing, storage, and exchange of personal data, creating significant challenges for privacy, accountability, and responsible data governance. Against this backdrop, the Digital Personal Data Protection Act, 2023 (DPDP Act) and the Digital Personal Data Protection Rules, 2025 (DPDP Rules) represent a significant transition from fragmented data-related regulation towards a dedicated statutory framework for digital personal data protection. Within this emerging framework, the principle of **Data Protection by Design** assumes particular significance as a preventive approach that seeks to integrate privacy and data-protection safeguards into organisational processes, technological systems, and data-processing practices from their inception rather than addressing risks after harm occurs. The constitutional foundation of such an approach can be traced to the recognition of privacy as a fundamental right under Article 21 and the broader doctrine of informational autonomy developed by the Supreme Court of India in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017).

This paper critically examines the emerging obligations relevant to Data Protection by Design under the DPDP framework and evaluates the extent to which the existing regulatory architecture facilitates preventive data governance. It analyses the responsibilities of Data Fiduciaries, including the adoption of reasonable security safeguards, organisational accountability, risk management, and measures aimed at preventing personal data breaches. The paper further identifies regulatory challenges arising from the absence of an explicitly articulated and comprehensive statutory model of "privacy by design," particularly concerning standardisation of compliance practices, technological accountability, regulatory oversight, and implementation by small and medium-sized entities. A comparative perspective with the General Data Protection Regulation (GDPR) is also employed to identify potential lessons for strengthening India's preventive data-protection architecture (European Parliament & Council of the European Union, 2016). The paper argues that effective Data Protection by Design requires clearer regulatory expectations, proportionate compliance mechanisms, technological safeguards, and stronger accountability standards. It concludes by proposing measures to develop a more preventive, risk-sensitive, and rights-oriented data protection regime in India.

Keywords: *Data Protection by Design; Digital Personal Data Protection Act, 2023; Data Fiduciaries; Privacy; Data Governance*

1. Introduction

1.1 Background and Evolution of Data-Driven Digitalisation in India

India's digital transformation has fundamentally altered the manner in which individuals, businesses, public authorities, and digital platforms interact with information. The expansion of smartphones, digital payments, e-commerce, social networking platforms, cloud computing, digital health services, online education, and digital public infrastructure has resulted in the continuous generation and processing of personal data. Personal information is no longer merely an administrative record; it has become an important economic, technological, and governance resource. Organisations

increasingly depend upon personal data to provide services, personalise user experiences, assess consumer preferences, detect fraud, develop artificial intelligence systems, and make commercial and administrative decisions.

The increasing significance of personal data has consequently transformed the relationship between individuals and organisations processing such information. Individuals frequently provide personal information as a condition for accessing digital services, while the actual collection, analysis, retention, sharing, and monetisation of that information may remain largely invisible to them. This creates an imbalance between the individual, who may have limited understanding of the subsequent use of their information, and the Data Fiduciary or other entity possessing the technical and organisational capacity to process it. Such asymmetry raises important questions concerning autonomy, transparency, accountability, and individual control over personal information.

The growth of India's digital economy has therefore generated a dual policy objective. On the one hand, regulation must facilitate technological innovation and the development of data-driven services. On the other, it must prevent unnecessary or disproportionate interference with individual privacy. The recognition of privacy as a constitutionally protected right has strengthened the legal basis for addressing these concerns. In *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), the Supreme Court of India recognised privacy as an intrinsic component of the rights to life, liberty, dignity, and autonomy. The judgment significantly altered the constitutional understanding of privacy by recognising that individuals have legitimate interests in controlling information concerning themselves.

The evolution of India's data protection framework must therefore be understood against this broader process of digitalisation. The Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 represented earlier attempts to regulate particular aspects of information security and sensitive personal information. However, the rapid expansion of digital technologies exposed limitations in a fragmented regulatory approach. The Justice B.N. Srikrishna Committee's report subsequently contributed to the development of a more comprehensive personal data protection framework (Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, 2018).

This regulatory evolution ultimately culminated in the **Digital Personal Data Protection Act, 2023 (DPDP Act)**. The Act seeks to establish a statutory framework governing the processing of digital personal data while attempting to balance individual privacy with legitimate purposes of data processing and the needs of India's digital economy. The subsequent **Digital Personal Data Protection Rules, 2025 (DPDP Rules)** further operationalise several aspects of the statutory framework.

Within this evolving regulatory environment, the question is no longer limited to what should happen after personal data has been misused or compromised. An equally significant question is whether privacy and data protection safeguards can be incorporated **before and during the design of technologies, services, and organisational processes**. This shift provides the foundation for examining Data Protection by Design.

1.2 Growing Risks Associated with the Collection and Processing of Personal Data

The extensive collection and processing of personal data creates benefits but simultaneously produces substantial risks. Modern digital systems can combine information obtained from multiple sources, allowing organisations to create detailed profiles of individuals. Data concerning identity, location, financial transactions, online behaviour, preferences, health, education, and professional activities may collectively reveal characteristics and patterns that individuals did not consciously intend to disclose.

One major concern is **function creep**, whereby information collected for one legitimate purpose is subsequently used for another purpose without adequate awareness or meaningful choice by the individual. The accumulation of large quantities of information also increases the consequences of unauthorised access, accidental disclosure, cyberattacks,

insider misuse, and other security failures. A data breach may expose individuals to financial loss, identity-related harms, discrimination, reputational damage, or persistent loss of control over their personal information.

The problem becomes more complex when personal data is processed through automated systems. Artificial intelligence and algorithmic technologies can analyse vast datasets to generate predictions, classifications, recommendations, or decisions concerning individuals. Such systems may create privacy risks even where the initial collection of information appeared lawful. The processing of seemingly ordinary information can generate sensitive inferences when multiple datasets are combined.

Consequently, effective data protection cannot depend exclusively upon individual vigilance. Requiring individuals to understand lengthy privacy policies, identify every possible future use of their data, and continuously monitor how organisations process their information places a disproportionate responsibility upon data principals. A meaningful privacy framework must therefore also impose responsibilities upon those designing and operating data-processing systems.

This provides a strong justification for a preventive regulatory approach in which privacy risks are identified and mitigated **at the design stage**, rather than only after a violation has occurred.

1.3 Emergence of Privacy-Oriented and Preventive Approaches to Data Governance

Traditional approaches to data protection have often focused on compliance with legal obligations after data has already been collected or processed. Such approaches may provide remedies, penalties, or corrective mechanisms following a violation. Although these mechanisms remain necessary, they are inherently limited when the objective is to prevent privacy harm before it materialises.

Preventive data governance seeks to alter this regulatory orientation. Instead of asking merely whether an organisation has violated a privacy rule, a preventive model asks whether privacy risks were identified during the planning, development, deployment, and modification of a data-processing activity. This approach treats privacy as an element of organisational governance and technological architecture rather than as an issue addressed exclusively by legal or compliance departments.

The concept is particularly significant in environments where data processing is embedded into the underlying architecture of digital services. Once a technological system has been developed around extensive data collection, modifying it at a later stage may be technically difficult and economically costly. Integrating privacy safeguards from the beginning can therefore reduce both regulatory risks and potential harm to individuals.

The preventive approach also reflects a broader movement in contemporary data protection law towards **accountability**. Organisations are increasingly expected not merely to comply with externally imposed rules but to demonstrate that appropriate systems, processes, safeguards, and governance structures exist to ensure compliance.

The European Union's General Data Protection Regulation (GDPR) provides an influential example. Article 25 expressly incorporates the principle of data protection by design and by default, requiring controllers to implement appropriate technical and organisational measures while considering factors such as the state of technological development, implementation costs, nature and purpose of processing, and associated risks (European Parliament & Council of the European Union, 2016).

India's emerging framework must consequently be examined to determine whether it similarly moves beyond reactive protection towards a preventive model.

2. Conceptualising Data Protection by Design

2.1 Meaning and Evolution of Data Protection by Design

2.1.1 Conceptual Origins

The intellectual foundation of Data Protection by Design can be traced to the broader concept of **Privacy by Design**, which emphasised the integration of privacy considerations into technological and organisational systems from their inception. Ann Cavoukian's influential framework presented Privacy by Design as an approach in which privacy is incorporated proactively rather than treated as an issue requiring remedial intervention after problems arise (Cavoukian, 2011).

The central premise is relatively straightforward: if a system is likely to process personal information, privacy considerations should form part of the system's architecture from the beginning. Privacy should not be treated merely as a document, policy, or contractual term. Instead, it should be reflected in the actual functioning of the system.

This approach becomes particularly important in contemporary digital environments because technological architecture can determine the practical extent of individual privacy. Decisions concerning what information is collected, how long it is retained, who can access it, whether it is encrypted, whether it can be linked with other datasets, and whether users can exercise meaningful control are frequently embedded in the design of digital systems.

Data Protection by Design consequently represents a movement from **privacy as an after-the-fact legal requirement** to **privacy as an ex ante governance principle**.

2.1.2 Privacy by Design versus Data Protection by Design

Although the expressions Privacy by Design and Data Protection by Design are often used interchangeably, an analytical distinction can be drawn between them.

Privacy by Design originated primarily as a broader governance and technological philosophy concerned with incorporating privacy considerations into systems and organisational practices (Cavoukian, 2011). **Data Protection by Design**, by contrast, has acquired a more explicit legal and regulatory dimension, particularly through the GDPR.

The distinction is important because data protection encompasses more than individual privacy. It also includes principles relating to lawful processing, transparency, accountability, security, data minimisation, purpose limitation, individual rights, and organisational responsibility.

Therefore, Data Protection by Design can be understood as the process of incorporating **legal, organisational, and technical data protection safeguards into the architecture and lifecycle of data processing**.

For the purposes of this paper, DPDP is understood broadly as an approach under which privacy and data protection risks are identified, assessed, and addressed during the design, development, deployment, and continued operation of systems that process personal data.

2.1.3 Preventive versus Reactive Approaches

The difference between preventive and reactive data protection can be represented as follows:

Reactive Approach	Preventive Approach
Responds after harm occurs	Identifies risks before harm occurs
Relies heavily on remedies and penalties	Emphasises risk mitigation
Privacy treated as compliance	Privacy integrated into system design

Reactive Approach

Focuses on violations

Primarily corrective

Often dependent on complaints or regulatory intervention

Preventive Approach

Focuses on preventing violations

Primarily anticipatory

Requires organisational responsibility

A reactive system remains essential because no regulatory architecture can eliminate every privacy risk. However, relying exclusively on penalties after a breach or misuse may be inadequate because certain privacy harms cannot easily be reversed. Once sensitive information has been publicly disclosed or widely disseminated, monetary compensation may not restore the individual's lost control.

DPDP therefore complements rather than replaces traditional enforcement. Its objective is to **reduce the probability and severity of harm before an infringement takes place.**

2.1.4 Role of Technology in Embedding Privacy Safeguards

Technology is not merely a source of privacy risks; it can also serve as an instrument of privacy protection. Technical measures such as encryption, access controls, authentication, pseudonymisation, data minimisation mechanisms, privacy-enhancing technologies, and secure deletion can reduce the exposure of personal information.

The technological dimension of DPDP is particularly important because legal principles cannot always determine how privacy should be implemented at a technical level. A legal obligation requiring reasonable security, for example, must ultimately be translated into organisational procedures and technological safeguards.

This creates a multidisciplinary character for DPDP. Effective implementation requires interaction between **law, technology, organisational governance, cyber security, risk management, and ethics.**

Accordingly, a legally compliant system should ideally incorporate privacy safeguards not only in its contractual documentation but also in its underlying technical architecture.

2.2 Core Principles of Data Protection by Design

2.2.1 Proactive Rather Than Reactive Measures

The first principle of DPDP is **proactivity**. Privacy risks should be anticipated before personal data processing begins. Organisations should identify foreseeable risks, determine appropriate safeguards, and continuously review whether those safeguards remain effective.

This changes the organisational question from:

“What should we do after a privacy breach?”

to:

“What can we build into the system so that the breach or misuse becomes less likely?”

Proactive protection therefore requires privacy considerations to be incorporated into planning, procurement, software development, data governance, employee training, and organisational decision-making.

2.2.2 Privacy as the Default

Privacy by default requires systems to operate in a manner that provides an appropriate level of privacy without requiring individuals to undertake complex additional actions.

The principle is important because users frequently accept default settings. If a platform automatically collects excessive information or makes extensive sharing the default option, the individual's formal ability to alter those settings may not constitute meaningful control.

Privacy-oriented defaults can therefore include:

- collecting only information necessary for the specified purpose;
- limiting access to personal information;
- restricting unnecessary data sharing;
- establishing appropriate retention periods; and
- providing privacy-protective settings from the outset.

The concept is particularly relevant to digital platforms where interface design can influence user behaviour.

2.2.3 Data Minimisation

Data minimisation requires organisations to avoid collecting or retaining personal information that is unnecessary for the relevant purpose. The principle is significant because the amount of data retained by an organisation can directly affect the magnitude of potential privacy and security risks.

If unnecessary information is never collected, it cannot subsequently be misused, leaked, or accessed without authorisation. Data minimisation therefore functions as both a **privacy principle and a risk-reduction mechanism**.

However, implementing minimisation can be challenging in data-driven business models where organisations may seek to collect information for future analytical or commercial purposes. This creates an important regulatory question concerning the boundary between legitimate future utility and excessive data collection.

2.2.4 Purpose Limitation

Purpose limitation requires personal data to be collected and processed in connection with specified and legitimate purposes. The principle seeks to prevent organisations from transforming information collected for one purpose into an unrestricted resource for unrelated activities.

From a DPbD perspective, purpose limitation should be incorporated into system architecture. Data-processing systems should ideally be designed so that access, use, and sharing correspond to authorised purposes.

Purpose limitation is especially important in environments involving artificial intelligence and large-scale analytics because datasets collected for one purpose may subsequently be valuable for unrelated predictive or algorithmic applications.

2.2.5 Transparency

Transparency is essential for meaningful data protection because individuals cannot exercise informed control over information they do not understand is being collected or processed.

A design-oriented approach therefore requires privacy information to be presented in an accessible and comprehensible manner. Transparency should not be reduced to lengthy legal notices that users rarely read. Instead, information concerning collection, purposes, retention, sharing, and user rights should be communicated in a manner appropriate to the nature of the service.

The challenge is to reconcile legal completeness with practical comprehension. Effective transparency therefore requires attention to **interface design, language, accessibility, timing, and context**.

2.2.6 Security Safeguards

Security constitutes an essential component of DPbD because weak technical architecture can expose personal information even when other legal requirements are formally satisfied.

Appropriate safeguards may include:

- encryption;
- access controls;
- authentication mechanisms;
- secure software development;
- monitoring and logging;
- vulnerability management;
- incident response mechanisms; and
- secure deletion.

The appropriate level of security should correspond to the nature and sensitivity of the data and the risks associated with its processing. A risk-sensitive approach avoids both under-protection and unnecessary compliance burdens.

2.2.7 User Control and Autonomy

A fundamental objective of data protection is to preserve the individual's meaningful ability to exercise control over personal information. DPbD can contribute to this objective by incorporating mechanisms that enable individuals to understand and manage their data.

User control may involve:

- accessible consent mechanisms;
- withdrawal mechanisms;
- correction procedures;
- deletion mechanisms where applicable;
- information about processing activities; and
- understandable privacy settings.

However, formal availability of these mechanisms does not necessarily guarantee meaningful autonomy. If withdrawing consent is substantially more difficult than providing it, or if users cannot understand the consequences of their choices, individual control may remain largely theoretical.

Therefore, DPDP should focus not simply on the **existence** of user controls but on their **usability and effectiveness**.

2.2.8 Accountability

Accountability provides the organisational foundation for DPbD. An organisation should be capable of demonstrating that it has considered privacy risks and implemented proportionate safeguards.

Accountability shifts data protection from a narrow legal-compliance function towards an organisational governance responsibility. It requires institutions to establish internal policies, assign responsibilities, document decisions, monitor compliance, and respond appropriately when risks emerge.

The accountability principle is particularly relevant to the DPDP framework because the effectiveness of India's data protection regime will depend significantly upon how Data Fiduciaries translate statutory responsibilities into organisational practices.

2.3 Theoretical Foundations of Data Protection by Design

2.3.1 Informational Self-Determination

The concept of **informational self-determination** provides an important theoretical basis for DPDP. It refers broadly to an individual's capacity to exercise meaningful control over information relating to themselves.

In the digital environment, however, individual control cannot depend entirely upon conscious decisions made by users. The complexity and scale of modern data processing make it difficult for individuals to monitor every transaction involving their information.

DPDP addresses this limitation by transferring part of the responsibility for privacy protection from the individual to the organisation designing and operating the data-processing system.

In the Indian constitutional context, the Supreme Court's recognition of informational privacy in *Puttaswamy* provides significant support for understanding personal information as connected with autonomy and dignity (*Justice K.S. Puttaswamy (Retd.) v. Union of India*, 2017).

2.3.2 Privacy as Autonomy

Privacy is closely connected with the capacity of individuals to make choices concerning their personal lives without unjustified interference. The Supreme Court's privacy jurisprudence links privacy with dignity, liberty, autonomy, and individual choice.

From this perspective, DPDP can be understood as an institutional mechanism for supporting autonomy. When systems are designed to minimise unnecessary collection, provide understandable choices, restrict unauthorised access, and facilitate individual control, they reduce the extent to which individuals are subjected to invisible or uncontrollable forms of data processing.

The significance of autonomy also demonstrates why privacy protection cannot be evaluated exclusively through the lens of economic harm. Loss of control over personal information may itself constitute a significant interference with individual autonomy.

2.3.3 Risk-Based Regulation

DPDP also reflects the logic of **risk-based regulation**. Not every data-processing activity creates identical risks. The potential consequences depend upon factors such as the nature of information, scale of processing, number of individuals affected, purpose of processing, technological complexity, and likelihood of misuse.

A risk-sensitive approach therefore requires organisations to identify and prioritise significant risks and implement safeguards proportionate to those risks.

This approach can make regulation more adaptable to technological change. Instead of prescribing identical safeguards for every organisation, regulators can require stronger measures where processing presents greater risks to individuals.

For India, this raises an important policy question: whether the DPDP framework should progressively develop more detailed risk-based standards for high-impact processing, artificial intelligence, children's data, large-scale profiling, and other emerging applications.

2.3.4 Accountability Theory

Accountability theory provides a further foundation for DPbD by emphasising that organisations processing personal data should be responsible for the consequences of their decisions.

Traditional regulatory models frequently focus upon determining whether an organisation has breached a particular rule. Accountability extends this approach by asking whether the organisation has established an effective system for preventing, identifying, documenting, and addressing privacy risks.

DPDP is therefore closely connected with organisational accountability because design decisions themselves can determine whether privacy risks are created or mitigated.

An accountability-oriented model would require organisations to demonstrate not merely that they have a privacy policy but that **privacy considerations actually influence technological and organisational decision-making**.

3. Constitutional and Jurisprudential Foundations of Data Protection by Design in India

3.1 Right to Privacy as the Constitutional Foundation

The constitutional development of privacy in India provides an important foundation for understanding the need for preventive personal data protection. Although the Constitution of India does not expressly employ the expression “data protection,” the right to privacy has been recognised as an intrinsic component of the fundamental rights framework. The constitutional recognition of privacy transformed the protection of personal information from a primarily statutory concern into an issue involving dignity, liberty, autonomy, and individual freedom.

The Supreme Court's decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) represents the central development in this regard. A nine-judge Bench unanimously recognised the right to privacy as a constitutionally protected right arising primarily from Article 21 and other guarantees contained in Part III of the Constitution. The Court rejected the understanding that privacy was merely a common-law or statutory interest and instead located it within the constitutional protection of individual liberty and dignity (*Justice K.S. Puttaswamy (Retd.) v. Union of India*, 2017).

The constitutionalisation of privacy has significant implications for personal data regulation. In a data-driven society, an individual's private sphere cannot be adequately protected merely by restricting physical intrusion. Information concerning a person's identity, relationships, activities, preferences, finances, location, health, and online behaviour can reveal intimate aspects of individual life. Consequently, informational privacy becomes an essential dimension of contemporary privacy protection.

From this perspective, Data Protection by Design can be viewed as a preventive mechanism for giving practical effect to constitutional privacy. If privacy is recognised as a constitutional value, legal protection should not be limited to providing remedies after information has been misused. The architecture through which personal information is collected and processed should itself incorporate appropriate safeguards.

3.2 Informational Privacy and Individual Autonomy

The concept of informational privacy occupies a particularly significant position in the Indian constitutional framework. The *Puttaswamy* judgment recognised that privacy encompasses an individual's interest in controlling information about themselves and protecting the ability to make autonomous decisions concerning personal life (*Justice K.S. Puttaswamy (Retd.) v. Union of India*, 2017).

Informational autonomy, however, becomes increasingly difficult to achieve in complex digital environments. Individuals routinely interact with applications, websites, platforms, financial systems, government portals, and digital services that process personal information through highly sophisticated technological infrastructure. The individual may technically provide consent, yet may not possess the practical capacity to understand every subsequent processing operation.

This creates an important limitation in purely consent-based approaches to privacy. If protection depends exclusively upon individuals making perfectly informed choices, the regulatory system places substantial responsibility upon persons who may lack the necessary technical knowledge or bargaining power.

Data Protection by Design responds to this structural problem by embedding safeguards within the systems responsible for processing personal data. Rather than requiring individuals to continuously protect themselves, organisations are expected to anticipate privacy risks and incorporate appropriate protections into their technological and organisational architecture.

Thus, DPDP can be conceptualised as an institutional complement to the constitutional principle of informational autonomy.

3.3 Privacy, Dignity and Data Protection

The relationship between privacy and dignity further strengthens the constitutional case for preventive data protection. The Supreme Court has repeatedly associated privacy with the dignity of the individual. Information concerning a person can affect how that person is perceived, treated, classified, or evaluated by others.

The consequences of personal data misuse therefore extend beyond financial loss. Unauthorised disclosure or inappropriate profiling can affect reputation, personal relationships, employment opportunities, access to services, and social participation. In certain circumstances, the processing of personal information may also facilitate discrimination or unjustified surveillance.

The protection of dignity consequently requires attention to the conditions under which personal information is collected and used. DPbD can support this objective by limiting unnecessary collection, restricting access, implementing appropriate security safeguards, and preventing information from being used beyond legitimate purposes.

The constitutional value of dignity therefore provides a normative justification for moving towards preventive rather than exclusively remedial data protection.

3.4 Proportionality and Data Processing

The constitutional principle of proportionality is also relevant to the design of data-processing systems. Privacy restrictions cannot be assessed merely by asking whether data processing serves a legitimate objective. The nature and extent of the interference with individual privacy must also be proportionate to the objective pursued.

In *K.S. Puttaswamy (Retd.) v. Union of India* (2017), the Court identified proportionality as an important component of constitutional analysis concerning privacy restrictions. A legitimate objective must therefore be pursued through means that bear an appropriate relationship to that objective and do not impose an excessive burden upon individual rights.

This principle has direct relevance to Data Protection by Design. If an organisation can achieve a legitimate objective without collecting particular categories of personal data, continued collection may raise questions concerning necessity and proportionality.

Similarly, if the same purpose can be achieved by retaining information for a shorter period, restricting access, anonymising information, or processing data locally rather than transferring it unnecessarily, privacy-protective design becomes a means of reducing the intensity of interference.

DPDP can therefore operationalise proportionality at the technological and organisational level.

4. Data Protection by Design under the Digital Personal Data Protection Act, 2023 and Rules, 2025

4.1 Introduction

The Digital Personal Data Protection Act, 2023 represents a significant development in India's approach to the regulation of digital personal data. It establishes a dedicated statutory framework governing the processing of digital personal data and allocates responsibilities among Data Principals, Data Fiduciaries, Data Processors, Consent Managers, and the regulatory authority. The Digital Personal Data Protection Rules, 2025 subsequently provide greater operational detail concerning several obligations established by the Act (Digital Personal Data Protection Act, 2023; Ministry of Electronics and Information Technology [MeitY], 2025).

The significance of this framework from the perspective of Data Protection by Design (DPbD) requires careful examination. Unlike the European Union's General Data Protection Regulation (GDPR), which expressly provides for “data protection by design and by default” in Article 25, the DPDP Act does not establish an identically titled, standalone statutory provision. This does not, however, mean that the Indian framework is entirely disconnected from the philosophy of preventive data protection. Several obligations imposed upon Data Fiduciaries can be interpreted as requiring privacy and security considerations to be incorporated into data-processing systems and organisational practices.

The central issue is therefore not whether the expression “Data Protection by Design” appears as an independent statutory provision, but **whether the combined architecture of the DPDP Act and Rules requires organisations to anticipate, prevent, and mitigate privacy risks through their technological and organisational arrangements.**

This distinction is important for evaluating the maturity of India's data protection regime. A framework based primarily upon post-violation remedies may address harm after it has occurred, whereas a design-oriented framework attempts to reduce the likelihood of harm at the point at which systems and processes are created. The DPDP framework contains several elements capable of supporting this preventive orientation, but their effectiveness depends upon interpretation, implementation, regulatory guidance, and institutional enforcement.

4.2 Evolution from Fragmented Regulation to a Dedicated Data Protection Framework

Before the enactment of the DPDP Act, India's regulation of personal information was dispersed across multiple legal instruments. The Information Technology Act, 2000 established the basic statutory framework for electronic transactions and cyber-related matters. Section 43A, together with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, addressed certain obligations concerning sensitive personal data.

Although these provisions represented an important regulatory step, they were developed within a broader information technology framework rather than a comprehensive personal data protection regime. The expansion of digital services, platform-based economies, online transactions, cloud computing, and data-driven technologies increasingly exposed the limitations of a fragmented approach.

The constitutional recognition of privacy further strengthened the need for comprehensive legislation. In *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), the Supreme Court recognised privacy as a constitutionally protected right and connected it with dignity, liberty, autonomy, and individual choice. The judgment provided an important normative foundation for subsequent developments in personal data regulation.

The Justice B.N. Srikrishna Committee subsequently proposed a comprehensive framework for protecting personal data while maintaining India's digital economy and innovation objectives (Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, 2018).

The enactment of the DPDP Act in 2023 therefore represents not simply another amendment to India's technology laws but a structural movement towards a dedicated personal data governance regime.

From the perspective of DPDP, this evolution is significant because comprehensive data protection legislation creates an opportunity to move beyond isolated security obligations towards **lifecycle-based governance of personal data**.

4.3 The Regulatory Architecture of the DPDP Act, 2023

The DPDP Act establishes several principal concepts that are directly relevant to Data Protection by Design.

4.3.1 Data Principal

The individual to whom the personal data relates is recognised as the **Data Principal**. The statutory recognition of the individual is important because it places the person, rather than the data itself, at the centre of the regulatory framework.

However, meaningful protection of Data Principals cannot depend entirely upon their ability to exercise statutory rights. Individuals may not possess the technical expertise necessary to evaluate the architecture of digital systems or identify risks associated with data processing.

DPbD therefore complements individual rights by requiring protective measures to be incorporated into the systems operated by Data Fiduciaries.

4.3.2 Data Fiduciary

The concept of the **Data Fiduciary** is particularly important for DPbD. A Data Fiduciary determines the purpose and means of processing personal data and therefore occupies a position of significant responsibility within the data-processing relationship (Digital Personal Data Protection Act, 2023).

The allocation of responsibility to the entity determining the purposes and means of processing creates an important foundation for preventive regulation. The organisation responsible for designing or determining the processing architecture is also the entity best placed to identify and mitigate risks arising from that architecture.

Accordingly, DPbD requires Data Fiduciaries to consider privacy implications throughout the data lifecycle rather than treating privacy as an issue that arises only when a complaint or breach occurs.

4.4 Lawful Processing and the Design of Data Collection

A fundamental requirement of data protection is that personal data should not be processed arbitrarily. The DPDP Act establishes a framework under which processing is linked to lawful grounds, including consent and certain legitimate uses recognised by the legislation (Digital Personal Data Protection Act, 2023).

From a DPDP perspective, this requirement should influence the architecture through which information is collected.

A privacy-oriented system should be capable of determining:

1. what personal data is being collected;
2. why it is being collected;
3. whether such collection is necessary;
4. the legal basis supporting processing;
5. how the information will be used; and
6. when the information should cease to be retained.

This demonstrates that lawful processing cannot be viewed exclusively as a legal-documentation requirement. It should also influence system design.

For example, if a digital service requires only a person's name and contact information to provide a particular service, the system should not automatically collect unrelated information merely because such information might have commercial value in the future.

The design question is therefore:

Does the technological architecture collect only what the identified processing purpose reasonably requires?

If the answer is negative, formal compliance with a privacy notice may not adequately address the underlying risk.

4.5 Consent Architecture and Data Protection by Design

Consent is one of the most important components of the DPDP framework. The Act requires consent to satisfy conditions relating to informed, specific, clear, and affirmative choice, and provides mechanisms through which consent can be withdrawn (Digital Personal Data Protection Act, 2023).

From the perspective of DPbD, consent should not merely be obtained; **the system through which consent is obtained should itself be privacy-protective.**

A poorly designed consent interface may technically obtain consent while undermining meaningful individual choice. Complex language, excessive information, pre-selected options, unclear consequences, or difficult withdrawal mechanisms can reduce the practical value of consent.

A design-oriented approach requires organisations to incorporate consent management into the architecture of their systems.

This includes:

- clear presentation of consent requests;
- separation of different processing purposes where appropriate;

- accessible information;
- easy withdrawal mechanisms;
- records of consent;
- mechanisms for updating consent;
- restrictions on processing following withdrawal where applicable.

The importance of this approach is reinforced by the DPDP Rules, 2025, which provide greater operational detail concerning consent mechanisms and Consent Managers (MeitY, 2025).

The emergence of Consent Managers is particularly significant because it can facilitate greater user control over consent decisions. However, the effectiveness of this mechanism will depend upon interoperability, accessibility, security, transparency, and public awareness.

Thus, the regulatory challenge is not merely to create a **legal right to consent**, but to design an environment in which consent can be meaningfully exercised.

4.6 Data Protection by Design and the Principle of Data Minimisation

Data minimisation represents one of the strongest conceptual connections between the DPDP framework and DPDP

The logic of minimisation is preventive: reducing unnecessary collection reduces the quantity of personal data exposed to potential misuse, unauthorised access, accidental disclosure, and security breaches.

A design-oriented implementation of minimisation requires organisations to examine data requirements at the beginning of a processing activity. Instead of designing a system around maximum possible data collection and determining restrictions later, organisations should begin with the question of **minimum necessary information**.

This approach becomes particularly important in commercial environments where personal information may have substantial economic value.

For example, an online educational platform may require limited information to provide access to a course. Collecting extensive behavioural, location, contact, or device information beyond what is necessary for the service could create additional privacy risks.

DPDP therefore encourages a shift from:

“How much data can the organisation collect?”

to:

“How little data can the organisation process while achieving the legitimate purpose?”

This represents a fundamental change in data governance philosophy.

4.7 Purpose Limitation and System Architecture

Purpose limitation is another important element of preventive data governance. Personal information collected for a particular purpose should not automatically become available for unrelated uses.

The risk of purpose expansion is particularly significant in artificial intelligence and big-data environments. Organisations may initially collect information for one service but later identify opportunities to use the same information for profiling, behavioural analysis, targeted advertising, automated decision-making, or AI development.

A DPDP approach requires purpose limitations to be reflected within technical architecture.

This may involve:

- role-based access;
- purpose-specific databases;
- restrictions on secondary use;
- controlled data sharing;
- access logs;
- processing permissions; and
- automated controls preventing unauthorised uses.

Thus, purpose limitation should operate not merely as a written organisational policy but as a **technical constraint on data processing**.

4.8 Security Safeguards and Preventive Data Protection

Security represents perhaps the most direct connection between the DPDP framework and DPbD.

The DPDP Act requires Data Fiduciaries to implement reasonable security safeguards to prevent personal data breaches (Digital Personal Data Protection Act, 2023). The DPDP Rules, 2025 provide additional detail concerning security measures and breach-related responsibilities (MeitY, 2025).

The significance of this requirement lies in its preventive character. The objective is not simply to respond to a breach but to establish safeguards that reduce the probability of unauthorised access or disclosure.

From a DPDP perspective, security measures may include:

- encryption;
- access controls;
- authentication mechanisms;
- secure software architecture;
- vulnerability testing;
- monitoring systems;
- incident detection;
- access logging;
- backup mechanisms; and
- secure deletion.

The regulatory challenge, however, lies in determining what constitutes “reasonable” security in a rapidly changing technological environment.

A rigid statutory list of technologies could quickly become obsolete. Conversely, excessively general requirements may leave organisations uncertain about the level of security expected from them.

A balanced approach should therefore combine **principle-based legislation with technologically adaptable regulatory guidance**.

4.9 Data Breach Prevention and Response

A data breach demonstrates the limitations of purely reactive approaches. Once personal data has been disclosed, the harm may be difficult or impossible to reverse.

The DPDP framework therefore combines preventive security obligations with breach-related notification and response mechanisms.

From a DPDP perspective, breach management should be incorporated into the system architecture before an incident occurs. Organisations should have mechanisms for:

1. detecting unusual access;
2. identifying compromised information;
3. restricting further access;
4. containing the incident;
5. documenting the breach;
6. notifying relevant stakeholders;
7. evaluating the consequences; and
8. preventing recurrence.

This represents an important shift from **incident response as an emergency function to incident preparedness as a design principle**.

An organisation that develops a system without considering how a breach would be detected or contained has not fully incorporated preventive data governance into its architecture.

4.10 Data Retention, Deletion and Lifecycle Management

Data protection should not end after collection. Personal data should be governed throughout its lifecycle.

Retention represents a significant risk because information maintained indefinitely remains vulnerable to future misuse, unauthorised access, or security failures.

A DPbD framework should therefore require organisations to incorporate retention periods and deletion mechanisms into system design.

Automated deletion can be preferable to purely manual processes because it reduces the possibility of human error and ensures that data does not remain stored simply because an employee failed to remove it.

Lifecycle management should therefore involve:

Collection → Use → Storage → Sharing → Review → Retention decision → Deletion

Each stage should involve appropriate safeguards.

The DPDP Rules, 2025 are particularly relevant in this context because they provide greater detail concerning obligations relating to retention and deletion in specified circumstances (MeitY, 2025).

4.11 Protection of Children's Personal Data by Design

Children's personal data requires heightened protection because children may have a limited understanding of the long-term consequences of sharing information online.

The DPDP Act establishes specific obligations concerning the processing of children's personal data, including requirements relating to consent and restrictions on certain forms of processing (Digital Personal Data Protection Act, 2023).

From a DPDP perspective, these requirements should be integrated into platform architecture.

A child-oriented service should, where applicable, incorporate:

- age-related safeguards;
- parental consent mechanisms;
- restrictions on targeted or harmful processing;
- child-friendly interfaces;
- limited data collection;
- enhanced security; and
- appropriate retention and deletion controls.

This illustrates the importance of moving beyond **paper compliance**. Simply including a clause concerning children in a privacy policy is insufficient if the technical architecture continues to permit inappropriate collection or processing.

4.12 Significant Data Fiduciaries and Enhanced Governance

The DPDP framework distinguishes certain Data Fiduciaries as **Significant Data Fiduciaries**, recognising that the scale and nature of some processing activities may create heightened risks.

This approach reflects a risk-based regulatory philosophy.

Organisations undertaking large-scale or high-impact data processing may require more sophisticated governance mechanisms because the consequences of failure can be substantially greater.

From a DPDP perspective, enhanced obligations for Significant Data Fiduciaries can support:

- systematic risk assessment;
- stronger security architecture;
- organisational accountability;
- independent evaluation;
- monitoring of processing practices; and
- Enhanced governance.

However, the effectiveness of differentiated regulation depends upon clear criteria and proportionate implementation.

The regulatory system should ensure that high-risk processing receives stronger safeguards without imposing unnecessary compliance burdens on low-risk activities.

4.13 Role of the Data Protection Board in Promoting DPDP

The Data Protection Board of India represents the institutional enforcement mechanism under the DPDP framework.

Its role is particularly important because principles such as accountability and reasonable security safeguards require interpretation and enforcement to become meaningful.

The Board can potentially contribute to DPDP through:

- enforcement decisions;
- interpretation of Data Fiduciary obligations;
- regulatory expectations;
- consideration of security failures;
- assessment of organisational compliance; and
- Development of jurisprudential standards.

Over time, enforcement decisions could clarify what constitutes adequate preventive protection.

For example, if the Board consistently considers whether an organisation had implemented reasonable safeguards **before** a breach occurred, it may encourage Data Fiduciaries to treat security and privacy as design-stage responsibilities.

The institutional effectiveness of the Board will therefore be a crucial determinant of whether India's framework develops into a genuinely preventive regime.

4.14 DPDP Rules, 2025: Operationalizing Preventive Data Governance

The DPDP Rules, 2025 are important because statutory principles require operational mechanisms if they are to influence organisational behaviour.

The Rules provide detailed requirements concerning several aspects of the Act, including security safeguards, personal data breach notifications, children's data, Consent Managers, Significant Data Fiduciaries, and other compliance mechanisms (MeitY, 2025).

From a DPbD perspective, the Rules can be understood as an important step towards translating broad legislative principles into organisational practices.

However, operationalisation should not be equated with complete standardisation. Data protection technologies evolve rapidly, and regulatory requirements must remain sufficiently flexible to accommodate innovation.

Consequently, India's regulatory model would benefit from a combination of:

Statutory principles + regulatory guidance + technical standards + organisational accountability + continuous review.

Such a model would provide flexibility while maintaining minimum levels of protection.

4.15 Explicit versus Implicit Recognition of Data Protection by Design

A central finding of this analysis is that the DPDP framework should be distinguished from the GDPR in terms of how DPbD is articulated.

The GDPR expressly states in Article 25 that controllers must implement data protection by design and by default (European Parliament & Council of the European Union, 2016).

The Indian framework does not employ the same explicit formulation as a standalone statutory principle. Instead, relevant elements are distributed across obligations concerning:

- lawful processing;
- consent;
- security safeguards;
- breach prevention;
- children's data;
- Data Fiduciary responsibilities;
- Significant Data Fiduciaries; and
- Related organisational measures.

This creates two possible interpretations.

First interpretation: Functional recognition

The DPDP framework may be understood as functionally incorporating DPbD because its substantive obligations require organisations to implement safeguards that can only be effectively achieved through appropriate system design.

Second interpretation: Regulatory incompleteness

Alternatively, the absence of an explicit DPbD provision may be regarded as a regulatory gap because organisations may lack a clear overarching standard requiring privacy considerations to be incorporated throughout the entire lifecycle of processing.

The second concern is particularly relevant for judicial and regulatory certainty. A clearly articulated DPbD principle would provide a coherent framework through which individual provisions could be interpreted.

4.16 Comparative Assessment with GDPR Article 25

The comparison with GDPR Article 25 demonstrates an important difference in regulatory philosophy.

The GDPR explicitly links design with data protection principles and requires consideration of factors including the state of technological development, implementation costs, the nature and purpose of processing, and risks to individuals (European Parliament & Council of the European Union, 2016).

India's approach is comparatively less explicit. Its statutory framework distributes preventive obligations across different provisions.

This may provide greater flexibility but can also create interpretive uncertainty.

Comparative Matrix

Dimension	GDPR	DPDP Framework
Explicit provision	DPbD Yes	Not expressed as an equivalent standalone provision
Privacy by default	Expressly recognised	Can be supported through broader obligations

Dimension	GDPR	DPDP Framework
Security	Detailed framework	principle-based Reasonable security safeguards
Data minimisation	Express principle	Reflected through purpose-oriented processing framework
Accountability	Explicitly developed	Reflected through Data Fiduciary obligations
Risk assessment	Stronger explicit architecture	More developing/indirect
Children's protection	Specific safeguards	Specific statutory protection
Regulatory authority	Independent authorities	supervisory Data Protection Board
Design-stage obligation	Explicit	Primarily derived from substantive obligations

The comparison suggests that India does not necessarily need to reproduce GDPR Article 25 word-for-word. Instead, it should develop an approach appropriate to India's legal, technological, economic, and institutional context.

4.17 Critical Assessment of the DPDP Framework

The DPDP framework represents a significant advancement in India's personal data protection landscape. Its emphasis on Data Fiduciary responsibility, security safeguards, consent, children's data, and institutional enforcement creates a foundation upon which preventive data protection can develop.

Nevertheless, several concerns remain.

First, the absence of an expressly articulated DPbD obligation may make it difficult to establish a uniform standard for design-stage privacy protection.

Second, the broad nature of certain obligations may result in inconsistent implementation among Data Fiduciaries.

Third, technological complexity may make compliance particularly challenging for organisations lacking specialised legal and technical expertise.

Fourth, the effectiveness of the framework will depend significantly upon the institutional capacity of the Data Protection Board and the development of regulatory guidance.

Finally, there is a risk that Data Protection by Design could become another documentation exercise unless regulators and organisations evaluate the **actual architecture and functioning of data-processing systems**.

Therefore, India's challenge is not simply to recognise privacy as a legal value but to translate that value into technological and organisational practice.

5. Emerging Obligations of Data Fiduciaries from a DPDP Perspective

5.1 Incorporating Privacy into Organisational Governance

Data protection cannot be effectively implemented through technical controls alone. Organisational structures must also allocate responsibility for privacy and security.

A Data Fiduciary adopting DPbD should ideally establish internal processes for identifying privacy risks, assessing new processing activities, monitoring compliance, and reviewing technological changes.

Privacy governance should consequently extend beyond the legal department. Product designers, software engineers, cybersecurity professionals, management personnel, and compliance teams may all influence how personal data is processed.

The design-oriented approach therefore promotes **privacy as an organisational culture rather than merely a regulatory obligation**.

5.2 Data Retention and Deletion

Retention practices constitute another important element of DPDP. Maintaining personal information indefinitely increases the period during which it may be exposed to unauthorised access or misuse.

A preventive framework should therefore incorporate retention controls into system architecture. Organisations should identify appropriate retention periods and ensure that mechanisms exist for deletion or disposal when information is no longer legitimately required.

Automated deletion mechanisms can be particularly valuable because they reduce dependence upon manual organisational action.

5.3 Protection of Children's Data

Children require enhanced protection because of their age, vulnerability, and potentially limited ability to understand the consequences of data processing.

The DPDP framework provides specific obligations concerning children's personal data. From a DPbD perspective, such requirements should be reflected in platform design rather than implemented merely through contractual terms.

Age-related safeguards, parental consent mechanisms where applicable, restrictions on harmful processing, and child-sensitive interfaces are examples of how legal requirements can be translated into system architecture.

This demonstrates that DPbD can serve as a bridge between **statutory protection and practical technological implementation**.

6. Comparative Perspective: India and the GDPR

The GDPR provides an important comparative benchmark because Article 25 expressly recognises **data protection by design and by default** (European Parliament & Council of the European Union, 2016).

Article 25 requires controllers to implement appropriate technical and organisational measures designed to implement data protection principles effectively and integrate necessary safeguards into processing. It also addresses data protection by default by requiring appropriate measures to ensure that only personal data necessary for the specific processing purpose is processed.

The Indian framework differs in its drafting approach. Rather than establishing a single comprehensive provision dedicated to DPbD, the DPDP Act and Rules distribute relevant responsibilities across different provisions.

This creates an important distinction:

GDPR model: explicit principle + detailed regulatory architecture.

DPDP model: dispersed obligations that may collectively support preventive protection.

The Indian approach has the potential advantage of flexibility. However, the absence of an expressly articulated DPbD standard may generate uncertainty regarding the precise expectations applicable to organisations.

7. Regulatory Challenges in Implementing Data Protection by Design in India

7.1 Lack of an Explicit and Comprehensive DPbD Standard

One of the principal challenges is the absence of a detailed statutory formulation equivalent to GDPR Article 25. While several provisions of the Indian framework can support preventive data protection, organisations may not always have a clear benchmark against which design practices can be evaluated.

7.2 Compliance Costs

Implementation of privacy-enhancing technologies, security controls, auditing mechanisms, and organisational governance may impose significant costs. These burdens may be particularly challenging for smaller enterprises.

7.3 Technological Complexity

The rapid development of artificial intelligence, cloud computing, Internet of Things technologies, biometric systems, and large-scale analytics makes it difficult for legislation to prescribe fixed technical solutions.

7.4 Lack of Technical Expertise

Effective DPbD requires professionals who understand both legal requirements and technological architecture. A shortage of interdisciplinary expertise may limit implementation.

7.5 Balancing Innovation and Privacy

Excessive regulation may discourage experimentation and technological innovation, whereas insufficient regulation may expose individuals to significant privacy risks. The regulatory challenge is therefore to establish safeguards proportionate to actual risks.

7.6 Enforcement Uncertainty

The practical effectiveness of DPbD ultimately depends upon regulatory supervision and enforcement. Without credible oversight, design-oriented obligations may become formal compliance exercises.

8. Critical Evaluation

The analysis demonstrates that India's emerging data protection regime contains several components compatible with the philosophy of Data Protection by Design. Security safeguards, organisational accountability, protection of children's data, consent mechanisms, and responsibilities imposed upon Data Fiduciaries can collectively contribute to preventive data governance.

However, there remains an important distinction between **having privacy-related obligations** and **having an expressly articulated Data Protection by Design regime**.

The DPDP framework therefore appears to provide a foundation for DPbD, but its practical effectiveness will depend upon regulatory interpretation, organisational implementation, technological standards, and enforcement.

The central challenge is to transform data protection from a compliance activity undertaken after system development into a principle influencing decisions **before personal data processing begins**.

9. Recommendations

India's DPDP framework can be strengthened through the following measures:

9.1 Explicit Recognition of DPDP

Future regulatory guidance should clearly articulate Data Protection by Design and by Default as an overarching compliance principle.

9.2 Sector-Specific Standards

Different sectors such as healthcare, banking, education, telecommunications, and digital platforms generate different privacy risks. Sector-specific guidance would therefore improve implementation.

9.3 Privacy-Enhancing Technologies

Regulatory policy should encourage encryption, pseudonymisation, anonymisation, access controls, secure computation, and other privacy-enhancing technologies.

9.4 Risk-Based Compliance

Compliance obligations should correspond to the scale, nature, sensitivity, and potential impact of data processing.

9.5 Support for MSMEs

Smaller organisations should receive practical compliance templates, technical guidance, model policies, and proportionate standards.

9.6 AI-Responsive Data Governance

Future regulatory development should address privacy risks created by automated decision-making, profiling, algorithmic inference, and large-scale AI systems.

9.7 Stronger Regulatory Guidance

The Data Protection Board and relevant governmental institutions should develop accessible guidance explaining how organisations can translate statutory principles into technological and organisational controls.

10. Conclusion

Data Protection by Design represents an important transition from reactive privacy protection towards preventive data governance. In an increasingly data-dependent economy, individuals cannot reasonably be expected to protect themselves against every consequence of complex and invisible data-processing operations. Responsibility must therefore also rest upon organisations that determine how personal information is collected, processed, stored, shared, and deleted.

India's DPDP Act, 2023 and Rules, 2025 establish an important foundation for this approach through obligations relating to Data Fiduciaries, security safeguards, accountability, consent, children's data, and other aspects of responsible data processing. Nevertheless, the framework does not yet articulate Data Protection by Design with the same explicitness and conceptual coherence found in Article 25 of the GDPR.

The future development of India's data protection regime should therefore focus on converting broad statutory principles into practical, risk-sensitive, and technologically adaptable design standards. Such an approach would enable privacy to become an integral feature of digital systems rather than a corrective measure applied after harm has occurred.

Ultimately, the effectiveness of India's data protection framework will depend not only upon the existence of statutory rights and regulatory institutions but upon whether **privacy is embedded within the architecture of India's digital ecosystem itself**.

References

1. Article 29 Data Protection Working Party. (2018). *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679*. European Commission.
2. Article 29 Data Protection Working Party. (2018). *Guidelines on transparency under Regulation 2016/679*. European Commission.
3. Bennett, C. J., & Raab, C. D. (2006). *The governance of privacy: Policy instruments in global perspective*. MIT Press.
4. Bygrave, L. A. (2014). *Data privacy law: An international perspective*. Oxford University Press.
5. Cavoukian, A. (2011). *Privacy by design: The 7 foundational principles*. Information and Privacy Commissioner of Ontario.
6. Committee of Experts under the Chairmanship of Justice B. N. Srikrishna. (2018). *A free and fair digital economy: Protecting privacy, empowering Indians*. Ministry of Electronics and Information Technology, Government of India.
7. De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., & Sanchez, I. (2018). The right to data protection in the era of the General Data Protection Regulation. *Computer Law & Security Review*, 34(2), 179–194.
8. De Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review*, 32(2), 179–194.
9. Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
10. Digital Personal Data Protection Rules, 2025, Ministry of Electronics and Information Technology, Government of India.
11. Edwards, L., & Veale, M. (2018). Enslaving the algorithm: From a “right to an explanation” to a “right to better decisions”? *IEEE Security & Privacy*, 16(3), 46–54.
12. European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. *Official Journal of the European Union*, L119, 1–88.
13. European Data Protection Board. (2020). *Guidelines 4/2019 on Article 25 data protection by design and by default*. European Union.

14. European Data Protection Board. (2021). *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*. European Union.
15. European Union Agency for Cybersecurity. (2023). *Data protection engineering: Technical guidance for implementing privacy and data protection by design*. European Union Agency for Cybersecurity.
16. Greenleaf, G. (2014). *Asian data privacy laws: Trade and human rights perspectives*. Oxford University Press.
17. Greenleaf, G. (2018). *Global data privacy laws 2017: 120 national data privacy laws, including Indonesia and Turkey*. Privacy Laws & Business International Report.
18. Kuner, C. (2017). *The General Data Protection Regulation: A commentary*. Oxford University Press.
19. Kuner, C., Bygrave, L. A., & Docksey, C. (Eds.). (2020). *The EU General Data Protection Regulation (GDPR): A commentary*. Oxford University Press.
20. Ministry of Electronics and Information Technology. (2025). *Digital Personal Data Protection Rules, 2025: Explanatory note*. Government of India.
21. Ministry of Electronics and Information Technology. (2023). *Digital Personal Data Protection Act, 2023: Frequently asked questions*. Government of India.
22. Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.
23. OECD. (2013). *The OECD privacy framework*. Organisation for Economic Co-operation and Development.
24. Regulation (EU) 2016/679, General Data Protection Regulation, art. 25, 2016 O.J. (L 119) 1.
25. Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.
26. Solove, D. J., & Schwartz, P. M. (2020). *Information privacy law* (7th ed.). Wolters Kluwer.
27. Spiekermann, S., & Cranor, L. F. (2009). Engineering privacy. *IEEE Transactions on Software Engineering*, 35(1), 67–82.
28. Tene, O., & Polonetsky, J. (2013). Big data for all: Privacy and user control in the age of analytics. *Northwestern Journal of Technology and Intellectual Property*, 11(5), 239–273.
29. Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, 7(2), 76–99.
30. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).