



INDIAN JOURNAL OF
LEGAL REVIEW

VOLUME 5 AND ISSUE 5 OF 2025

INSTITUTE OF LEGAL EDUCATION



INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN – 2583-2344

(Open Access Journal)

Journal's Home Page – <https://ijlr.iledu.in/>

Journal's Editorial Page – <https://ijlr.iledu.in/editorial-board/>

Volume 5 and Issue 5 of 2025 (Access Full Issue on – <https://ijlr.iledu.in/volume-5-and-issue-5-of-2025/>)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 – info@iledu.in / Chairman@iledu.in



ILE Publication House is the
**India's Largest
Scholarly Publisher**

© Institute of Legal Education

Copyright Disclaimer: All rights are reserve with Institute of Legal Education. No part of the material published on this website (Articles or Research Papers including those published in this journal) may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher. For more details refer <https://ijlr.iledu.in/terms-and-condition/>

LEGAL FRAMEWORK GOVERNING AI AND DATA PROTECTION

AUTHOR – ANSA ELCY ALEX, STUDENT AT AMITY LAW SCHOOL

BEST CITATION – ANSA ELCY ALEX, LEGAL FRAMEWORK GOVERNING AI AND DATA PROTECTION, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (5) OF 2025, PG. 598-604, APIS – 3920 – 0001 & ISSN – 2583-2344

ABSTRACT

Digital Personal Data Protection Act (DPDP Act): A New Era for Data Protection in India

The DPDP Act (Digital Personality Personal Data Protection), 2023, represents an important step in regulating data protection in the country. The aim is to protect individual personal data and at the same time, ensuring that advances in businesses and technological developments, including artificial intelligence (AI), can thrive responsibly. In contrast to the European Union's

General Data Protection Ordinance (GDPR), which includes detailed guidelines for AI-related data processing, the DPDP Act is not explicitly mentioned. However, principles and obligations apply to AI-controlled data processing, which presents important legal and regulatory challenges. In 2022, the Indian government introduced the Digital Personal Data Protection Act (DPDP Act), a comprehensive law to protect the personal data of Indian citizens. The law is a major change in India's approach to data protection, highlighting the need for transparency, accountability and user consent.¹¹⁶⁹ The DPDP Act determines several important provisions that must be compliant with the organization that processes personal data. These include Memos and Approvals: Organizations must clearly and accurately notify you of a clear and accurate notice of the collection and use of personal data and obtain consent before processing such data.¹¹⁷⁰

Minimizing Data: Organizations simply collect and process personal data necessary for the purposes specified in the communication.¹¹⁷¹

Data Protection according to Draft and Standard Settings: Organizations must implement data protection principles and protection measures throughout the lifecycle of their personal data and ensure that the standard settings for products and services are privacy.¹¹⁷²

GRASP - EDUCATE - EVOLVE

¹¹⁶⁹ Digital personal data protection act, 2022 (india)

¹¹⁷⁰ Digital personal data protection act, 2022 (india) section 5

¹¹⁷¹ Digital personal data protection act, 2022 (india) section 6

¹¹⁷² Digital personal data protection act, 2022 (india) section 7

1.1 KEY PRINCIPLES OF THE DPDP ACT AND ITS IMPACT ON AI

The DPDP Act is based on the fundamental principles of data protection, accountability and transparency that directly impact AI applications. Some of the key aspects include: Consulting based data processing: The DPDP Act provides that data carriers (the organizations that collect and process personal data) must obtain consent from individuals (data managers) before processing data. Those who rely on AI systems, particularly machine learning models trained on huge data records, face the challenge of obtaining explicit consent, especially when data is used for purposes beyond the individual's initial understanding.¹¹⁷³ However, DPDP enforces the desired restrictions. This means that data can only be used for the specific purposes that were collected. This could prevent AI developers from resilient data for innovation and creating friction between data protection laws and AI research.¹¹⁷⁴ AI controlled companies, particularly those in sectors such as healthcare, banking and social media, can be exposed to lower obligations and stricter compliance, including data testing and risk reviews AI applications, particularly those using automated decision making, must address these requirements.¹¹⁷⁵ For example, AI based credit ratings or AI facial recognition systems should ensure that individuals can question themselves about their impact. Indian AI startups and multinational technology companies could face preliminary problems. Approach to AI The DPDP approach also addresses the use of artificial intelligence (AI) in the processing of personal data. The law recognizes the potential benefits of AI, but also recognizes risks associated with its use, such as distortion, discrimination, and lack of transparency. Organizations need to ensure AI systems are transparent and can receive clear and accurate information about their use of AI in the processing of personal data.¹¹⁷⁶ The law provides for penalties for noncompliance,

¹¹⁷³ Digital Personal Data Protection Act, 2023, Section 6 (Consent Framework).

¹¹⁷⁴ DPDP Act, 2023, Section 4 (Purpose Limitation).

¹¹⁷⁵ DPDP Act, 2023, Section 10 (Significant Data Fiduciary Obligations).

¹¹⁷⁶ Digital Personal Data Protection Act, 2022 (India), Section 15

liance, including a fine of upto 'crores (approximately \$6.7 million) or a company's company of 2%. The focus of the law on transparency, accountability and user consent determines new standards for data protection in India. His approach to AI recognizes the potential benefits of this technology, and at the same time recognizes the risks associated with its use.¹¹⁷⁷ AI is carefully accepted. The DPDP Law approach as AI continues to transform industry, revolutionizes our lives and ways of working, documenting the need for a nuanced approach to DPDP law. The AI, DPDP Act requires companies to assess their effectiveness before using AI systems and processes personal data. These reviews should identify and evaluate the potential risks and consequences of AI use, including the risk of distortion, discrimination and damage to people. decision making. The three organizations should ensure that the AI system provides clear and accurate information about the data used for training, the algorithms used, and the decisions determined. This transparency is important to build trust in AI systems and to help individuals understand how personal data is used. Make decisions that have a major impact on the individual.¹¹⁷⁸

1.2 OVERVIEW OF GDPR AND ITS IMPLICATION FOR AI

The General Data Protection Ordinance (GDPR), issued by the European Union in 2018, is generally considered to be one of the most comprehensive data protection laws in the world. It has been developed to protect the personal data and privacy of people in the digital world. This regulation applies to all organizations that process personal data from EU residents, regardless of where the organization is based.¹¹⁷⁹ GDPR aims to enable people with stronger control over their personal information by determining strict guidelines for data collection, storage and processing. Organizations must obtain the individual's express consent before processing the data and must clearly communicate how the data is used. Furthermore, the rules emphasize data

¹¹⁷⁷ Digital Personal Data Protection Act, 2022 (India), Section 16

¹¹⁷⁸ Digital Personal Data Protection Act, 2022 (India), Section 15-19

¹¹⁷⁹ (GDPR Summary) <https://www.gdprsummary.com/gdpr-summary/>

minimization. This means that you should only collect data that is needed for a particular purpose. These principles are particularly relevant in the context of AI where large amounts of data are often processed to train algorithms. One of the most important effects of GDPR on AI is its impact on automated decision making and profiling. Article 22 of the GDPR gives an individual the right not to be determined solely by automatic processing and includes

profiling, as it requires that the algorithm be transparent, explainable and unbiased. For AI developers, this means that data protection and security are considered at every stage of the AI lifecycle, from data collection to algorithm supply.¹¹⁸⁰ This approach not only improves compliance, but also provides trust with user. These rights allow individuals to control their data and take into account the organization. Questions about the assurance of these rights are raised in the case of AI systems, especially when it involves complex algorithms and large data sets. By promoting ethical data practice and transparency, regulation is not only effective, but also encourages the development of trustworthy AI systems. Organizations prioritize GDPR.¹¹⁸¹

1.2.1 Principles of AI and GDPR:

The General Data Protection Regulation (GDPR) rests on key tenets encompassing lawfulness, fairness, and transparency, as well as purpose limitation, data minimization, accuracy, storage limitation, integrity, and accountability. These principles are designed to guarantee the protection of individual rights concerning the handling of their personal data. However, artificial intelligence (AI) applications, especially those utilizing machine learning, predictive analytics, and facial recognition, face significant hurdles in adhering to these principles. A particular challenge arises from the tendency of AI systems to gather and process data for unforeseen purposes, often conflicting

with the principles of purpose limitation and data minimization.¹¹⁸²

1.2.1 Exploring Automated Decision Making and the Right to Explanation

One of the most discussed aspects of GDPR related to AI is Article 22, which grants individuals the right to make automated decisions, including profiles, if such decisions have a legal or significant effect.¹¹⁸³ This means that AI-based credit ratings, configuration algorithms, or facial recognition systems must include human supervision or clear justification. The AI model, especially Deep Learning Systems, acts as a "black box", making it difficult to give wise explanations about decisions. This creates legal uncertainty and practical challenges for AI businesses.¹¹⁸⁴

1.2.2 The right to participate and compatibility

GDPR grants several rights via personal data. These rights represent the challenges of AI-controlled applications, especially for those using big data analytics. For example, AI systems trained with personal data may be difficult to implement the "right to forget" because deleting the data used in training may not completely remove the impact on the AI model (Article 17). Furthermore, the right to data portability (Article 20) requires that AI systems provide individual in a structured form. This can be difficult when AI is coagulated and converted in complex.¹¹⁸⁵

1.2.3 The fairness and discrimination of AI

systems can be increased by inheriting existing distortions in training data. The GDPR emphasizes fair processing and prohibits discrimination based on sensitive data such as breed, gender, and political opinions (Article 9). This means that AI developers need to ensure that their algorithms do not achieve unfair or biased results. However, ensuring AI fairness is technically complicated. This is because distortions can be embedded deep in the data records, making them difficult to delete. Regulators are increasingly needing algorithm audits and fairness review to mitigate the

¹¹⁸⁰ (the impact of GDPR in artificial intelligence)
<https://securiti.ai/impact-of-the-gdpr-on-artificial-intelligence/>

¹¹⁸¹ (The impact of GDPR ON AI)
https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU%28020%29641530

¹¹⁸² GDPR, Article 6 (Lawfulness of Processing).

¹¹⁸³ GDPR, Article 22 (Automated Decision-Making and Profiling).

¹¹⁸⁴ GDPR, Articles 15-21 (Data Subject Rights).

¹¹⁸⁵ GDPR, Article 20 (Right to Data Portability)

se risks.¹¹⁸⁶

1.2.4. Data Security and AI Risks

In AI systems that process personal and sensitive data, strict safety requirements of the GDPR (Article 32,34) are involved. AI applications need to conduct strong encryption, anonymization and risk reviews to prevent data injuries, particularly in healthcare, financial and law enforcement authorities. Furthermore, GDPR privacy requires design and default (Article 25) (Article 25), and the AI system can integrate data protection measurements at all stages of development. This is a challenge for businesses looking to coordinate innovation with compliance.

1.2.5 Cross-border data transmission and globalization

Many AI companies are working on global and process data from users in several jurisdictions. The GDPR restricts the transmission of crossborder data to countries that do not have appropriate data protection laws (Articles (40-50)

This affects AI companies that train models using international data records or rely on cloudbased AI services. Companies must obtain legal mechanisms such as SCC (Contract Clauses)¹¹⁸⁷ Binding Enterprise Rules (BCRs) to comply with the GDPR data transfer rules.

1.2.5. GDPR

The future of AI regulation within the framework of the GDPR forms a strong basis for AI governments, but AI challenges such as Deepfake, generative AI, and autonomous decisionmaking do not pose completely. The EU is working on AI laws that complement the GDPR by determining clear rules for highrisk AI applications. Future AI regulations will introduce stricter requirements for algorithm transparency, accountability and fairness, allowing the design of legal environments for the processing of AI-controlled data.¹¹⁸⁸

1.3 KEY PRINCIPLE OF GDPR AND DPDP ACT IN AI REGULATION

General Data Protection Ordinance (GDPR) and the Digital Personal Data Protection Act 2023 (DPDP Act) represent two important framework conditions in the field of data protection. The GDPR is a global benchmark for data protection, but the DPDP Act reflects India's TaylorMade approach to protecting personal data in socioeconomic contexts. Together, they provide valuable insight into responsible AI regulation. The GDPR regulations stipulate that personal data must be processed legally and fairly, and provide clear communication about individuals about how they use it. Similarly, it is a DPDP Act consentbased processing, requiring individual explicit and informed consent before data is processed. For AI systems, this means that data recording and use is transparent, ethically well discovered, and encourages trust among users. Another general principle is Minimizing the data The GDPR requires companies to collect only the data needed for a particular purpose, and the DPDP Act enforces similar restrictions to prevent excessive data collection. This principle is particularly relevant to AI where large data records are often used to train algorithms. By adhering to data minimization, businesses can reduce the risk of abuse and improve compliance. The GDPR is responsible for ensuring compliance with that principle, but the DPDP Act refers to the "data lath" and organizations responsible for protecting personal data.¹¹⁸⁹ For AI developers, this means that robust governance mechanisms are implemented and regular audits are conducted to ensure ethical practices. Article 22 grants an individual the right not to make a decision based solely on automated processing if such a decision has a significant effect. Although the DPDP Act does not explicitly relate to automated decisionmaking, its focus on transparency and accountability indirectly supports ethical AI practices. This underscores the need for an explanatory AI system that can justify user decisions. The GDPR requires businesses to integrate data protection measures into their systems from the sta

¹¹⁸⁶ GDPR, Article 9 (Processing of Special Categories of Personal Data).

¹¹⁸⁷ GDPR, Articles 25, 32-34 (Security and Privacy by Design).

¹¹⁸⁸ European Commission, Proposal for the AI Act (2021)

¹¹⁸⁹ (Article what are the 7 principle of GDPR) <https://www.gdpreu.org/7-main-data-protection-principles-under-gdpr/>

rt. For AI, this means that dataprotection and security features are included in the algorithm, ensuring compliance with the entire AI lifecycle. While the GDPR sets a global standard, the DPDP method provides a localized perspective that addresses India's unique challenges. Together they underscore the importance of installing technological advances with privacy and accountability, paving the way for a safe, integrated digital future.¹¹⁹⁰

1.4 EXTRA TERRITORY APPLICATION AND CROSS BORDER DATA TRANSFER REGULATION

In our interconnected world, data transcends geographical limitations, effortlessly traversing international lines through various digital channels such as cloud platforms, email systems, mobile applications, and online resources. However, the laws dictating data governance are confined within national territories, creating a discrepancy. To address this disparity, numerous legal systems have broadened their scope to encompass data processing activities occurring outside their national perimeters, a principle referred to as extraterritorial application. Concurrently, regulations concerning cross-border data transfers have become paramount in safeguarding personal information, ensuring its protection even after it crosses the originating country's border. These two legal principles hold particular importance within the realm of Artificial Intelligence (AI), where AI models are frequently developed using extensive data collections sourced from global users. This section will delve into the implications of extraterritorial application and cross-border transfer regulations for AI developers and organizations involved in managing personal data. Extraterritoriality allows a country's laws to be applied beyond its geographical boundaries. In data protection, this means that organizations based outside a country must still adhere to its privacy laws if they process the data of its residents. For example, a US-based AI

company providing services to Indian users is obligated to comply with India's data protection laws, even without a physical presence in India.¹¹⁹¹ Prominent examples of extraterritorial application in data protection include:

- General Data Protection Regulation (GDPR): Article 3 extends the GDPR's reach to data controllers and processors located outside the EU if they offer goods or services to, or monitor the behaviour of, individuals within the EU¹¹⁹². Like the DPDP Act, the GDPR also extends its reach beyond its borders by regulating entities that process the data of EU residents, even if those entities are located outside the EU.
- Section 3(e) of India's Digital Personal Data Protection Act (DPDP Act), 2023, extends the Act's jurisdiction beyond India's borders, stipulating that it applies to the processing of personal data related to offering goods or services to individuals within India, regardless of where the processing occurs. This means that even foreign entities that process data in connection with offering goods or services to individuals in India are subject to the DPDP Act's provisions.¹¹⁹³ The California Consumer Privacy Act (CCPA) applies to businesses that collect data from California residents, irrespective of whether the business is physically located within California.¹¹⁹⁴

The fragmented nature of international data laws necessitates a commitment to universal protection of personal data, regardless of the processing location. Organizations developing and deploying AI models cannot use geographical

¹¹⁹⁰ (Role of AI in DPDP act transforming data privacy in india) <https://corridalegal.com/role-of-ai-in-dpdp-act/>

¹¹⁹¹ Kuner, Christopher (2015). Extraterritoriality and regulation of international data transfers in EU data protection law. *International Data Privacy Law*, 5(4), 235-245 <https://doi.org/10.1093/idpl/ipv019> last visited on 13/2/2025

¹¹⁹² GDPR Article 3 – Territorial Scope.

¹¹⁹³ DPDP Act 2023, Section 3(e) – Application of the Act to processing in connection with offering goods or services to data principals in India

¹¹⁹⁴ California Consumer Privacy Act (CCPA), Section 1798.140(c)

distance to evade accountability. This is crucial because AI models trained on global data must adhere to a complex web of legal requirements.¹¹⁹⁵

1.4.1 Cross-border data transfer regulations.

Which is designed to maintain a consistent level of privacy protection for personal data, even when it is transferred internationally. These regulations are of paramount importance for AI systems, which often rely on cloud infrastructure deployed across various geographic regions¹¹⁹⁶.

1.4.2 GDPR's Approach to Cross -Border Transfer.

The GDPR significantly restricts the transfer of personal data outside the EU/EEA, permitting such transfers only under specific circumstances: first, if the European Commission has recognized the destination country as providing an adequate level of data protection¹¹⁹⁷; second, if appropriate safeguards are implemented, such as Standard Contractual Clauses or Binding Corporate Rules; or third, if the transfer is justified by a specific derogation, for instance, explicit user consent or the necessity for fulfilling a contract. To illustrate, if an AI analytics platform located in India processes data of EU residents, it must rely on Standard Contractual Clauses unless the EU Commission grants India an adequacy decision¹¹⁹⁸.

1.5 INDIA'S APPROACH UNDER ACT , 2023

India's Data Protection Approach Under the DPDP Act, 2023:

The Digital Personal Data Protection (DPDP) Act, 2023 governs international data transfers, granting the Central Government the power to

restrict cross-border data flow via notifications, particularly to countries deemed to lack "adequate protection."

Key Points:

- The Act does not impose a complete ban on international data transfers; however, the government retains the authority to create blacklists or require approvals.
- Data fiduciaries are responsible for ensuring that international data processors adhere to equivalent data protection standards.
- The Indian legal framework prioritizes governmental oversight of data destinations over individual company security measures.¹¹⁹⁹

Sector Specific and Bilateral Consideration Beyond national legal frameworks:

- Specific industries, such as finance and healthcare, are subject to more stringent export control regulations regarding sensitive information.
- Nations might establish bilateral or multilateral accords, such as the EU-U.S. Data Privacy Framework, to support secure and reliable data transfers¹²⁰⁰

Implication for AI Developers and Organization

For AI Developers and Organizations: Navigating the Complexities of Global AI Regulation

The interwoven nature of extraterritorial application and data transfer restrictions creates significant compliance obligations for AI companies with international operations.

Core Challenges:

- Reconciling disparate legal frameworks (e.g., aligning GDPR with the Indian DPDP Act).

¹¹⁹⁵ Wu, Weiyue, and Liu, Shaoshan (2023). A Comprehensive Review and Systematic Analysis of Artificial Intelligence Regulation Policies. arXiv <https://doi.org/10.48550/ARXIV.2307.12218> last visited on 10/02/2000

¹¹⁹⁶ Weber, R. H. (2013). Transborder data transfers: concepts, regulatory approaches and new legislative initiatives. *International Data Privacy Law*, 3(2), 117-130 <https://doi.org/10.1093/idpl/ipt001> last visited on 10/02/2000

¹¹⁹⁷ Phillips, Mark (2018). International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR). *Human Genetics*, 137(8), 575-582 <https://doi.org/10.1007/s00439-018-1919-7> last visited on 10/02/2025

¹¹⁹⁸ GDPR Chapter V – Transfers of personal data to third countries or international organisations

¹¹⁹⁹ DPDP Act 2023, Section 16 – Transfer of personal data outside India

¹²⁰⁰ European Commission (2023). Adequacy decisions and international data flows – EU-U.S. Data Privacy Framework

- Integrating region-specific privacy mechanisms within AI systems.
- Enforcing data localization mandates for sensitive data types like biometric or financial information.
- Developing thorough Data Processing Agreements (DPAs) and transfer impact assessments.

Illustrative Scenario: Consider a facial recognition firm processing data of Indian citizens but utilizing servers in Singapore; the company must ensure Singapore's data protection standards are on par with India's, or risk legal repercussions under Indian law.

Recommended Compliance Approaches:

- Conduct comprehensive data flow mapping to pinpoint international data transfers.
- Employ modular AI designs to isolate sensitive data processing within specific regions.
- Leverage privacy-enhancing technologies such as encryption and federated learning.
- Maintain continuous monitoring of government announcements and legal shifts across relevant jurisdictions.
- Meta (facebook) and GDPR :Due to concerns regarding data transfers from the EU to the US, Meta encountered legal obstacles and substantial fines under GDPR, ultimately necessitating the storage of European user data on servers within the EU.¹²⁰¹
- Tik Tok in India :Citing privacy issues and geopolitical factors, India prohibited TikTok and numerous other applications, highlighting the impact of data localization and sovereignty on AI governance.¹²⁰²

¹²⁰¹ Court of Justice of the European Union, Schrems II Case (C-311/18) – Invalidation of the EU-U.S. Privacy Shield

¹²⁰² Press Information Bureau, Government of India (2020). Ban on Chinese apps over data security concerns