VOLUME 5 | ISSUE 4

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

SAFEGUARDING DIGITAL PRIVACY: AN IN-DEPTH ANALYSIS OF INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT, 2023

- Mansi Soni[1]

ABSTRACT

In today's digitally driven world, data privacy has emerged as a cornerstone of individual rights and societal well-being. With the proliferation of digital transactions, educational admissions, healthcare services, and property dealings, the collection and handling of sensitive personal data have become unavoidable. However, this vast repository of information is often susceptible to misuse, creating significant risks for individuals. Recognizing these challenges, the Ministry of Electronics and Information Technology ("**MeitY**") introduced the Digital Personal Data Protection Act, 2023 ("**DPDP Act**") and its accompanying Rules, drafted on January 03, 2025. This legislative framework aims to balance innovation with robust data protection measures. The DPDP Act introduces groundbreaking provisions such as explicit parental consent for processing children's data and stringent requirements for safeguarding sensitive data like financial records and health information. It aligns with global data privacy status & methods, particularly the European Union's General Data Protection Regulation ("**GDPR**"), in catering to India's unique socio-economic landscape.This research paper delves into the DPDP Act's key features, including its focus on data principals' rights, obligations of data fiduciaries, and mechanisms for redressal in case of breaches. It also explores the broader implications for businesses and institutions, especially in the financial and healthcare sectors, which increasingly rely on digital agreements and transactions. The paper critically examines the act's capacity to mitigate privacy risks amidst concerns over government oversight and enforcement.Furthermore, a comparative analysis is conducted between the DPDP Act and international data protection frameworks, with a focus on the GDPR, the California

[1] Visiting Faculty at Amity University, Gwalior

© 2025 International Journal of Advanced Legal Research

Consumer Privacy Act ("**CCPA**"), and other prominent privacy laws. This analysis provides insight into how India's approach aligns with and diverges from global best practices, and the potential challenges of harmonizing international data protection standards.Ultimately, the study underscores the DPDP Act's potential to shape India's data protection regime, fostering trust in digital ecosystems while addressing the pressing need for accountability in an era where data is both an asset and a vulnerability.

Key words: Data Privacy, Fiduciaries, Privacy Laws, GDPR.

INTRODUCTION

As technology is developing at unprecedented pace in this interconnected digital age, data plays a pivotal role in innovation as well as in economic growth of the individuals. Every digital or online interaction contains digital footprints which are derived from the data incurred by the individuals who usually get involved in e-commerce, online banking or transactions, using cashless payment applications or taking healthcare schemes such as life insurance or health insurance policies. Such data are coined as sensitive personal data which can be forged or challenge the privacy of the person by intermediating that data. With the growth of digital facilities, it is quite difficult to secure the personal or primary data which needs to be filled for enjoying the perks of the internet. However, global regulations GRDP & Indian regulation DPDP Act tries to confront these critical challenges by imposing the landscape of the issue faced and balancing utility of these perks which needs to be protected by proper authority[2]. It also made efforts to dive into web security to safeguard data privacy, examining the mechanism of interplay between societal needs, technological advancements & aspects of legal framework by spotting gaps & required recommendations. Many inquisitive individuals had expected that the rules would broaden the DPDP Act's justification in regards with the process of personal data[3]. Nevertheless, the consent-centric framework is unaltered because the rules didn't elaborate new basis for commercial companies to process non- consent. By offering fresh guidelines for consent notices, the rules support the consent first strategy which must provide independent information of others, necessitating a modification in the practice of amalgamating consent with acceptance of

[2]Sarif, S. M. (2024). Complete set of the journal. *IIUM Journal of Case Studies in Management*, *15*(1).
[3]*Ibid.*

© 2025 International Journal of Advanced Legal Research

terms & conditions[4]. It's still unclear if this only makes an entreaty to data that has been accumulated or if it is applicable to data obtained from behavioural monitoring. Despite this uncertainty, companies should make building thorough data inventories a top priority in order to guarantee compliance and lucidity. Additionally, these inventories will aid the creation of concise and understandable consent notifications[5]. The Indian government has made draft regulations available for public review 16(*sixteen*) months after DPDP Act was commenced. These regulations are intended to operationalize & elucidate important legal requirements[6]. However, no grounds are available to revoke consent if it was not the base for processing personal data & the processing was carried out for a legitimate purpose, with the unusual situations as mentioned under **Section 7(a)** of the DPDP Act which requires voluntary consent to process personal sensitive data. Processing of personal information outside India is governed by **Rule 14** of the DPDP Rules. As it declares the limitations & compliance criteria set by the Indian government will apply to the collection & usage of private data protected by DPDP Act.[7] Further the central government is currently in charge of defining and enforcing these standards & prohibitions as they are not yet specified in the draftDPDP Rules. At the first presentation of the DPDP Act, 2023 it faced a lot of market speculation as the central government had compiled it as a '*negative list*' as the other authorities of several nations use the personal data but determined countries forbid from transferring or treating personal data[8].

OBJECTIVES

1. To protect the Digital Personal Data of the citizens by providing legal implications.
2. To enhance Data Principles with proper guidelines and rules for the usage of Data collected by the individuals.
3. To impose restrictions regarding sharing of Data with unauthorised persons in order to safeguard breach of privacy or to create accountability with the fiduciaries to protect their fiduciary data by maintaining reasonable security.

[4]*Ibid.*
[5]*Ibid.*
[6]*Ibid.*
[7]Malhotra, C., & Bhilwar, A. (2023). Striving to build citizens' trust in the digital world. In *Routledge eBooks* (pp. 141–161).
[8]*Ibid.*

© 2025 International Journal of Advanced Legal Research

4. To obtain required consent before approaching for the personal data from every person even from the variant sensitive classes such as children & differently abled people.
5. To embrace the upcoming challenges in introducing the rules regarding the violation of Digital Data Privacy.

METHODOLOGY

This doctrinal research on **Digital Personal Data Protection** employs a method of qualitative study, concentrating on a detailed examination of the current legal regulation controlling data privacy and protection. This research adopts a desk-based study which entails a thorough analysis of accessible literature, legislative texts, court judgements & other relevant documents. The research approach is intended to allow for an in-depth comparative analysis of the legislative framework around **digital data privacy & protection in India**. This comparative analysis aims to identify areas of convergence and divergence between Indian and global data protection standards, offering insights into potential improvements and best practices. The research focuses on the obstacles & complications connected with the implementation of these legislative provisions. The report dives into crucial concerns such as consent mechanism, data fiduciary duties & data principal rights. It also explores how emerging technologies, such AI present new issues to personal data protection.Further the research assesses the practical consequences of the DPDP Act & Rules for a variety of consumers, including corporations, government organisations and people. It seeks to give a detailed knowledge of how these laws affect data governance, corporate compliance tactics, & the overall goal of preserving individual's privacy rights in the digital era. Additionally, to main legal materials, the research makes use of secondary sources such as journals, reports, expert views, regulatory authority reports & cases laws analysis.

UNDERSTANDING DIGITAL PRIVACY

With more than 80 (*eighty*) crore internet users, India is one of the nations that uses & generates capital the most per person. For millions of Indians, digital India has changed their lives which as a result concerned about the security or privacy of personal data have emerged

© 2025 International Journal of Advanced Legal Research

as crucial elements of everyday interactions & have been discussed extensively in a variety of settings in recent years. In ***Justice K.S. Puttaswamy v. Union of India***[9] a nine-judge bench uphold the basic right to privacy guaranteed by the Indian Constitution to every person in India and certain laws has also been provided with its reasonable restrictions[10].Digital privacy includes the appropriate handling, processing, storing & sharing of the personal data, it also includes how technology, market speculation, methods of data collection & the legal structures regulates the interactive activities digitally[11]. The exponential growth in the amount & diversity of personal digital data being gathered & handled in the digital era has made data privacy even more important in recent years. However, there are some significant ways to understand the need of data privacy:[12]

- Guarantees the privacy & security of private information, including transactional records, medical records, private correspondence;
- Upholds the trust by ensuring the appropriate data handling as it creates and maintains fiduciary relationship between person and the association;
- Assuring that laws and regulations for safeguarding confidential data are followed properly; and
- Guarding from unauthorised use of identity, fraud or misrepresentation by illegal spying or other misuses of personal data[13].

In order to comply with data privacy regulations, businesses should collect as limited data as possible on their customers. Only explicit, unambiguous and lawful purposes should be pursued when collecting sensitive data, and those purposes should not be compromised by subsequent processing.[14] Businesses should only collect data that they intend to use for certain objectives.[15] Such a doctor's office will need the patient's weight, height, age and medical conditions in order to provide services to a particular person whereas in case of buying insurance policy the company will require to obtain information such as family

[9] *Justice K.S. Puttaswamy v. Union of India 494 of 2012, (2017) 10 SCC 1*. (n.d.). Retrieved January 22, 2025,
[10] *Ibid.*
[11] Introduction to Data privacy/ Data Privacy: Understanding its importance in the Digital Age |RSMIndia. (n.d.). *RSM India*
[12] *Ibid.*
[13] *Ibid.*
[14] What is data privacy? (n.d.). *Geeks for Geeks*
[15] What is data privacy? (n.d.). *Geeks for Geeks.*

© 2025 International Journal of Advanced Legal Research

details, family income, etc[16]. Information about an person's race, culture, political views, religion, inheritance, facial recognition, health information, gender identity or life is deemed confidential and is protected by stronger laws under the European Union's GDPR[17]. Data security, which is associated with data confidentiality, is concerned with keeping data out of the hands of unauthorised users [18]. People who regularly provide their private information to companies must also understand data privacy and its consequences, as must negotiating a complicated regulatory environment. Businesses are rapidly gathering information on their users which aims to achieve the purpose of learning more about their customers and opening up new avenues for value creation. The previous two years saw the creation of 90% (*ninety percent*) of data used or collected from the users. People's inquiries are yielding more accurate findings & vital industries like hospitals are seeing improvements in the experiences of patients[19]. However, a clear security strategy, encryption, secure connections such as Virtual Private Networks ("**VPNs**") for sending sensitive data and safety precautions by keeping IT facilities on site and burning critical paper documents are all used to achieve this[20]. Moreover, to protect these digital personal data of individuals, different organisations and agencies have introduced their principles for the safety and security of such data produced by the people. The three principles of America's Central Intelligence Agency ("**CIA**") i.e. confidentiality, availability and integrity should be followed by organisations while protecting sensitive data or information in general[21]. European Union's GDPR[22] states seven basic principles for data privacy which are:

- Lawfulness, transparency & fairness
- Limited access of data to organisations
- Narrow down the approaches
- Less accurate information
- Safety & security

[16] *Ibid.*
[17] *Ibid.*
[18] *Ibid.*
[19] Tobin, D. (2025, January 8). *What is Data Privacy—and Why Is It Important?* Integrate.io.
[20] What is data privacy? (n.d.). *Geeks for Geeks.*
[21] *Ibid.*
[22] *Regulation - 2016/679 - EN - gdpr - EUR-Lex.* (n.d.).

© 2025 International Journal of Advanced Legal Research

- Control over storage of data
- Data governance

These principles elaborate the ways to use, share, communicate to service providers or to safeguards approaches made by the consumers. According to the study of these principles the first principle examines how businesses get private information and establishes an unambiguous demand that such techniques must be lawful & have explicit privacy policies and goals. Companies need to explain why they need your personal information and how they plan to utilize it. The second principle, aims to guarantee that the firms only gather information pertinent to the current job. In essence, businesses are not allowed to retain data merely because they may need it in the future. To help establish a possible contributor for their endeavour, a corporation could ask for basic details such as name, email, profession. In the unlikely scenario that the company's digital records hacked this approach also serves as a means of limiting access and personal harm[23]. Third principle highlights that private information cannot be gathered for study and subsequently shared with the promotional or market management team for advertising. This concept ensures to guarantee privacy and prevent businesses from using personal data for their own good instead of specific agreements made. According to the fourth principle, if any organisation requires to obtain the personal data of the customer, they must mention the accurate need of that particular information or ask for the mandatory data only and it must be a reasonable requirement.[24] Principle fifth makes sure that inquiry teams refrain from keeping or utilizing personal information for purposes other than for which it was originally intended. Commonly to the security concept, this GDPR's principle of integrity & confidentiality organisation must ensure that proper safety mechanisms are established to safeguard the personal information they possess.[25] The European Union's GDPR discussed the adequate technical & organisational strategies which further includes implementing technological and safety procedures, performing risk assessments for data security. Further sixth and seventh principles of digital data privacy stated that businesses have no right to keep the data in their

[23] Introduction to Data privacy/ Data Privacy: Understanding its importance in the Digital Age |RSMIndia. (n.d.). *RSM India*.
[24] Introduction to Data privacy/ Data Privacy: Understanding its importance in the Digital Age |RSMIndia. (n.d.). *RSM India*.
[25] Introduction to Data privacy/ Data Privacy: Understanding its importance in the Digital Age |RSMIndia. (n.d.). *RSM India*.

© 2025 International Journal of Advanced Legal Research

database for any further utilisation after the completion of the required transaction of documents or data required for the work, they must obscure or remove the information[26]. If any organisation wishes to utilize any data for the new cause or events they must obtain the consent of the person and proceed with it and must maintain the documentation prepared to defend your strategy.[27]

REGULATIONS GOVERNING DIGITAL PERSONAL DATA & UNDERSTANDING GLOBAL PERSPECTIVE

The eagerly anticipated DPDP Act[28] has been enacted by the Indian Parliament. The DPDP Act is India's initial extensive data protection law, and it was commenced in the country's official notification in the gazette on August 11, 2023. It will further update the current patchwork of laws pertaining to the protection of personal data. Similar to the EU's GDPR the DPDP Act covers the entire handling of digital personal data in India and in some cases, has extraterritorial reach[29]. The Indian Telecommunications Act, 2002 ("**IT Act**") [30], the Digital India Act, 2023[31]& the National Data Governance Policy[32] are among the other new digital policy efforts that will coexist with the DPDPAct[33]. According to the IT Act there are two primary classifications into which the data falls i.e. Personal Data & Sensitive Personal Data[34], as it defines the data as an expression of knowledge, facts, information, subject matter or formalised way which stored internally in the database or intended to be examined in an automated system[35]. In addition to IT Act[36], The Indian Constitution and rules of Sensitive

[26]*Ibid.*
[27] Introduction to Data privacy/ Data Privacy: Understanding its importance in the Digital Age |RSMIndia. (n.d.). *RSM India*.
[28]*THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 (NO. 22 OF 2023)* (2023rd ed.). (n.d.). [English].
[29] Digital-personal-data-protection-Act-Indias-new-data-protection-framework.pdf. (n.d.). *DPDP Act,2023*.
[30]Parliament of India. (2023). THE TELECOMMUNICATIONS ACT, 2023. In *THE TELECOMMUNICATIONS ACT, 2023*.
[31]Digital India Dialogues. (2023). Digital India Act, 2023. In *Digital India Dialogues.*
[32]*National Data Governance Framework Policy posted on: 27 JUL 2022 2:44 PM by PIB Delhi*. (2022, July 27). Retrieved January 22, 2025, from
[33] Digital-personal-data-protection-Act-Indias-new-data-protection-framework.pdf. (n.d.). *DPDP Act,2023*.
[34] SIngh, A. (2020, June 25). Brief note on SPDI. *Privacy Protection - India*.
[35] SIngh, A. (2020, June 25). Brief note on SPDI. *Privacy Protection - India*.
[36]Government of India. (2000). THE INFORMATION TECHNOLOGY ACT, 2000. In *THE INFORMATIONTECHNOLOGY ACT, 2000*.

© 2025 International Journal of Advanced Legal Research

Personal Data & Information Rules[37] ("**SPDI Rules**") guarantees the freedom of speech and expression & right to personal liberty under **Article 19**&**Article 21** respectively which implies every citizen to express themselves. In ***Kharak Singh v. State of Uttar Pradesh***[38] The Supreme Court observed that although the right to privacy is a basic right, there are some limitations based on substantial common good[39]. According to **Rule 3** of SPDI Rules bank account information,passcodes,biometrics etc falls under the category of sensitive data. Furthermore, the foundation for data protection in India has been the IT Act[40]& the SPDI Rules[41] until the DPDP Act[42] and DPDP Rules are put into effect. `The DPDP Act will have a significant impact on many foreign companies that operate in India, depend on India's service agencies or category suppliers for their services, or are aiming to enter the Indian economy, [43]as India has the fifth-highest GDP in the world and one of the fastest-growing digital markets. The earlier drafts of the DPDP Act is a unique legal system which differs significantly from the GDPR even if it draws influence from it[44]. Asia witnessed the quick change in the legal environment regarding the concept of data protection as complete data protection legislation has lately been passed in several nations such as China,Thailand,Indonesia & Sri Lanka[45]. All of these nations took preventive measures towards breach of data privacy by pertaining clauses or reflecting internationally the comprehensive privacy laws in the region's rising trend.[46] The particular clauses or methods of implementation of these regulations differ greatly, demonstrating the disparate approaches taken by Asian nations regarding data safety and security. Moreover, North America's California Consumer Privacy Act ("**CCPA**")[47] imposed duties on companies and rights on consumers with relation to the gathering, selling and use of personal data. In order to protect

[37]Government of India, MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY, & Department of Information Technology. (2011). *Information Technology (Electronic Service Delivery) Rules, 2011*.
[38] (1963) AIR 1295 1964 SCR (1) 332
[39] SIngh, A. (2020, June 25). Brief note on SPDI. *Privacy Protection - India*.
[40] Government of India. (2000). THE INFORMATION TECHNOLOGY ACT, 2000. In *THE INFORMATION TECHNOLOGY ACT, 2000*.
[41]Government of India, MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY, & Department of Information Technology. (2011). *Information Technology (Electronic Service Delivery) Rules, 2011*.
[42] Digital-personal-data-protection-Act-Indias-new-data-protection-framework.pdf. (n.d.). *DPDP Act,2023*.
[43] What is India's Digital Personal Data Protection Act (DPDPA) 2023? (n.d.). *RSM INDIA*.
[44]What is India's Digital Personal Data Protection Act (DPDPA) 2023? (n.d.). *RSM INDIA*.
[45]Simmons, D. (n.d.). *17 Countries with GDPR-like Data Privacy Laws*.
[46]Mishova, A. (2024, October 23). *Data protection Laws around the world: A Global perspective*. GDPR Local.
[47] CALIFORNIA CONSUMER PRIVACY ACT OF 2018. (2025). In *cppa.ca.gov* (pp. 1–65).

© 2025 International Journal of Advanced Legal Research

consumer data, the CCPA presents new compliance requirements for companies doing business in California or aiming to reach California customers[48]. By passing privacy and safety regulations, 120 (*One Hundred and Twenty*) nations worldwide have acknowledged the need of safeguarding private information.[49] These laws seeks to protect private information in general class of the society by giving data subject rights and requiring organisations that handle data to guarantee the safety and appropriate management of personal information, with an emphasis on permission, privacy safeguards and accountability the fundamental tenets of these legislation frequently mirror those of significant framework such as GDPR of European Union and the various data protection statues of the U.S.A.[50]Organisations that operate in several countries may find it challenging to adhere to all of the privacy rules and regulations in each of those nations. The GDPR enforces strict regulations, including the need to designate a data protection officer in specific businesses, the demand to inform authorities about incidents involving data instantly and the need to maintain confidential documents of safeguarding actions.[51] The enormity and expense of regulatory adherence are increased by these particular requirements, which require firms to comply, evaluate,preserve and show conformity[52]. It is anticipated that the data protection regulatory landscape will only get stricter in the future.[53] More stringent enforcement of privacy regulations is anticipated, particularly with regard to highly confidential data such as health and child information. The Children Online Privacy Protection Act[54] in the United States of America is undergoing revisions to strengthen the duty of care and stiffen fines for infractions involving children's data. Data protection regulations face both possibilities and problems as a result of the deployment of new technology. By claiming complete control on data supplied to the third-party platforms or the use of servers to solve out or improve

[48] Mishova, A. (2024, October 23). *Data protection Laws around the world: A Global perspective*. GDPR Local.
[49]*Ibid.*
[50] Mishova, A. (2024, October 23). *Data protection Laws around the world: A Global perspective*. GDPR Local.
[51] Mishova, A. (2024, October 23). *Data protection Laws around the world: A Global perspective*. GDPR Local.
[52]Simmons, D. (n.d.). *17 Countries with GDPR-like Data Privacy Laws*.
[53]*Ibid.*
[54]*15 USC 6501: Definitions*. (n.d.).

© 2025 International Journal of Advanced Legal Research

compliance approach[55]. But there are hazards associated with having less insight into the distribution of customer's information which calls for strong compliance procedures and rules[56]. Additionally, AI Technologies are growing more laws pertaining to artificial intelligence which are passed globally as legislators attempt to strike a balance between protecting customer's rights and promoting technical advancement[57].

CONCLUSION & SUGGESTIONS

In conclusion, the evolving landscape of data privacy laws presents both challenges and opportunities. With proactive measures, informed decision-making, and global collaboration, governments, businesses, and individuals can collectively navigate the complexities of data protection. By embracing this legal evolution, societies can build a foundation of trust, ensure privacy, and unlock the transformative potential of the digital economy responsibly and sustainably. The optimism lies in the shared goal of balancing innovation with privacy, ensuring a secure digital future for all. Data privacy regulations, both in India and globally, aim to strike a balance between fostering technological advancements and safeguarding individual rights. Laws like the DPDPA and the European Union's General Data Protection Regulation (GDPR) share similar objectives, such as ensuring transparency, lawful data handling, and protecting sensitive personal information. However, they differ in their approach. While the GDPR is known for its comprehensive and stringent provisions, the DPDPA takes a more localized perspective, addressing India's unique digital ecosystem and economic priorities. This comparative flexibility makes the DPDPA well-suited to the Indian context, where digital growth must be harmonized with privacy protection. Globally, more than 120 countries have enacted privacy laws to address the challenges posed by rapid digitalization. Frameworks such as California's Consumer Privacy Act (CCPA) and Asia's emerging data protection laws reflect the universal recognition of the importance of data privacy. These laws vary in their scope and application, yet they converge on core principles such as transparency, accountability, and user consent. The global movement toward stricter data protection demonstrates a shared commitment to safeguarding personal information in the face of evolving threats, such as unauthorized data access, misuse, and breaches. Despite

[55]Mishova, A. (2024, October 23). *Data protection Laws around the world: A Global perspective*. GDPR Local.
[56]Mishova, A. (2024, October 23). *Data protection Laws around the world: A Global perspective*. GDPR Local.
[57]*Ibid.*

© 2025 International Journal of Advanced Legal Research

these challenges, the future of data privacy is optimistic. With a growing emphasis on compliance, businesses are now more aware of their responsibilities to protect customer data. Measures such as limited data collection, secure storage, and transparent usage policies build trust between organizations and individuals. Moreover, the integration of advanced technologies like encryption and artificial intelligence offers promising tools to enhance data security. At the same time, these technologies present new regulatory challenges, prompting lawmakers worldwide to adapt and refine their legal frameworks.

Suggestions on DPDP Rules:

The Digital Personal Data Protection (DPDP) Rules require several enhancements to ensure clear compliance while maintaining business flexibility. Firstly, clear compliance guidelines, especially around data security, retention, and breach notifications, should be introduced to reduce ambiguity. A risk-based approach for cross- border data transfers, along with certification-based mechanisms, would balance security with operational flexibility.A phased implementation timeline (12-24 months) is needed to allow businesses time to adapt before enforcement. A tiered penalty structure should also ensure penalties are proportional, particularly for SMEs. Sector-specific guidelines should address unique compliance needs in industries like banking and healthcare to prevent overlaps with existing Regulations. SMEs should be provided simplified compliance frameworks to reduce regulatory burdens. Harmonizing the rules with global standards like GDPR will facilitate smoother cross-border operations. Flexibility in breach notification timelines, as well as recognizing implied consent for routine transactions, can further ease compliance. Employee data processing should not require repeated consent for routine HR tasks. Guidelines for emerging technologies like AI and blockchain should support innovation while safeguarding privacy.

Finally, focusing training on data-heavy roles rather than all employees will ensure more efficient use of resources. These changes will help create a more balanced and effective data protection regime that fosters both privacy and business growth.

REFERENCES

JOURNALS

© 2025 International Journal of Advanced Legal Research

- Sarif, S. M. (2024). Complete set of the journal. *IIUM Journal of Case Studies in Management*, *15*(1). https://doi.org/10.31436/ijcsm.v15i1.240
- Digital-personal-data-protection-Act-Indias-new-data-protection-framework.pdf. (n.d.). *DPDP Act,2023*. https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2023/08/digital-personal-data-protection-act-indias-new-data-protection-framework.pdf
- *15 USC 6501: Definitions.* (n.d.).https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim

ARTICLES

- Introduction to Data privacy/ Data Privacy: Understanding its importance in the Digital Age |RSMIndia. (n.d.). *RSM India*. https://www.rsm.global/india/insights/consulting-insights/importance-of-data-privacy
- SIngh, A. (2020, June 25). Brief note on SPDI. *Privacy Protection - India*. https://www.mondaq.com/india/privacy-protection/956252/brief-note-on-spdi
- Simmons, D. (n.d.). *17 Countries with GDPR-like Data Privacy Laws*. https://insights.comforte.com/countries-with-gdpr-like-data-privacy-laws
- Mishova, A. (2024, October 23). *Data protection Laws around the world: A Global perspective*. GDPR Local. https://gdprlocal.com/data-protection-laws-around-the-world-a-global-perspective/
- What is India's Digital Personal Data Protection Act (DPDPA) 2023? (n.d.). *RSM INDIA*. https://www.rsm.global/india/insights/consulting-insights/guide-to-digital-personal-data-protection-act
- Tobin, D. (2025, January 8). *What is Data Privacy—and Why Is It Important?* Integrate.io. https://www.integrate.io/blog/what-is-data-privacy-why-is-it-important/
- What is data privacy? (n.d.). *Geeks for Geeks*. https://www.geeksforgeeks.org/what-is-data-privacy/

BOOKS

© 2025 International Journal of Advanced Legal Research

- Malhotra, C., & Bhilwar, A. (2023). Striving to build citizens' trust in the digital world. In *Routledge eBooks* (pp. 141–161). https://doi.org/10.4324/9781003433194-6

CASES

- *Justice K.S. Puttaswamy v. Union of India 494 of 2012, (2017) 10 SCC 1*. (n.d.). Retrieved January 22, 2025, from https://indiankanoon.org/doc/127517806/
- *Kharak Singh v. State of Uttar Pradesh* (1963) AIR 1295 1964 SCR (1) 332 https://main.sci.gov.in/judgment/judis/3641.pdf.

REGULATIONS

- *Regulation - 2016/679 - EN - gdpr - EUR-Lex*. (n.d.). http://data.europa.eu/eli/reg/2016/679/oj
- *15 USC 6501: Definitions*. (n.d.). https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim
- *THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 (NO. 22 OF 2023)* (2023rd ed.). (n.d.). [English]. https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
- Digital-personal-data-protection-Act-Indias-new-data-protection-framework.pdf. (n.d.). *DPDP Act,2023*. https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2023/08/digital-personal-data-protection-act-indias-new-data-protection-framework.pdf
- Parliament of India. (2023). THE TELECOMMUNICATIONS ACT, 2023. In *THE TELECOMMUNICATIONS ACT, 2023*. https://www.indiacode.nic.in/bitstream/123456789/20101/1/A2023-44.pdf
- Digital India Dialogues. (2023). Digital India Act, 2023. In *Digital India Dialogues*. https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf
- *National Data Governance Framework Policy posted on: 27 JUL 2022 2:44 PM by PIB Delhi*. (2022, July 27). Retrieved January 22, 2025, from https://pib.gov.in/PressReleasePage.aspx?PRID=1845318

© 2025 International Journal of Advanced Legal Research

- Government of India. (2000). THE INFORMATION TECHNOLOGY ACT, 2000. In *THE INFORMATION TECHNOLOGY ACT, 2000*. https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf
- Government of India, MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY, & Department of Information Technology. (2011). *Information Technology (Electronic Service Delivery) Rules, 2011*. https://www.meity.gov.in/sites/upload_files/dit/files/RNUS_CyberLaw_15411.pdf
- What is India's Digital Personal Data Protection Act (DPDPA) 2023? (n.d.). *RSM INDIA*. https://www.rsm.global/india/insights/consulting-insights/guide-to-digital-personal-data-protection-act
- CALIFORNIA CONSUMER PRIVACY ACT OF 2018. (2025). In *cppa.ca.gov* (pp. 1–65). https://cppa.ca.gov/regulations/pdf/ccpa_statute.pdf

© 2025 International Journal of Advanced Legal Research