



INTERNATIONAL LAW  
JOURNAL

---

**WHITE BLACK  
LEGAL LAW  
JOURNAL  
ISSN: 2581-  
8503**

*Peer - Reviewed & Refereed Journal*

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

[WWW.WHITEBLACKLEGAL.CO.IN](http://WWW.WHITEBLACKLEGAL.CO.IN)

## **DISCLAIMER**

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal

– The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

WHITE BLACK  
LEGAL

## **EDITORIAL TEAM**

### **Raju Narayana Swamy (IAS ) Indian Administrative Service officer**



Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) ( with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and diploma in Public

a professional Procurement from the World Bank.

### **Dr. R. K. Upadhyay**

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM-degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.





## **Senior Editor**

### **Dr. Neha Mishra**



Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

### **Ms. Sumiti Ahuja**

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.



### **Dr. Navtika Singh Nautiyal**

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.



### **Dr. Rinu Saraswat**

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

### **Dr. Nitesh Saraswat**

E.MBA, LL.M, Ph.D, PGDSAPM

Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.

More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.



### **Subhrajit Chanda**

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

## ***ABOUT US***



WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

W H I T E   B L A C K  
L E G A L

# DATA PROTECTION AND PRIVACY

## CHALLENGES IN DIGITAL AGE IN INDIA

AUTHOR NAME: - NIVEDITA SINGH

### INTRODUCTION

In the rapidly evolving landscape of the 21<sup>st</sup> century, the interplay between technology and law has become increasingly intricate and pervasive. As technological advancements continue to reshape our societies, legal frameworks are challenged to adapt, ensuring that the rights and responsibilities of individuals and entities are upheld in this digital age.

The relationship between law and technology is complex and multifaceted. At the most elementary level, technology consists in the application of labour to create a product, to generate a service or otherwise to produce a desired result. Technology develops as ways are found to produce new results or to produce old results using fewer or less costly inputs. Law is generally understood to exist as a set of rules adopted by a society's governing institutions that are applicable to all of its inhabitants. Law and technology interact when legal rules foster or retard the development of technology. They also interact when society decides that technology produces undesirable results and employs legal rules to contain or modify those results.

The relationship between law and technology is constantly evolving as new technologies emerge and new legal challenges arise. One of the most significant legal implications of the digital age is the issue of privacy, with the vast amount of personal data that is collected and stored by companies, governments, and other entities, there is a growing concern about the protection of that data. Regulatory challenges in data protection and privacy in the digital age in India stem from the rapidly evolving technological landscape and emerging privacy concerns.

- i. Technological Advancements:** - The swift pace of technological progress introduces complexities in regulating new technologies like artificial intelligence (AI) and the Internet of Things (IoT), requiring continuous updates to privacy laws to keep pace with innovation.
- ii. Cross-Border Data Transfers:** - Balancing the flow of data for international business operations with data protection requirements poses an ongoing challenge. Ensuring

compliance with regulations on cross-border data transfers while safeguarding personal information adds complexity to data protection efforts.

- iii. **Government Surveillance:** - The balance between government surveillance for national security and individual privacy remains a contentious issue. Establishing transparent surveillance laws and clear procedures for government access to individuals' data is crucial to prevent misuse and protect privacy rights.
- iv. **Social media and E-Commerce:** - The popularity of social media platforms and e-commerce websites raises concerns about user data privacy, data sharing practices, targeted advertising, and securing financial information in online transactions. Protecting children's online privacy is also a critical aspect that requires attention within the digital landscape.
- v. **Cybersecurity Threats:** - Incidents of cybersecurity breaches continue to be a concern, emphasizing the need for robust security measures to prevent unauthorized access to personal data. Staying current on cybersecurity best practices is essential to strengthen defences against potential breaches.

## LAWS IN INDIA

In India, data protection and privacy are governed by several key laws and regulations, including:

1. **Digital Personal Data Protection Act, 2023 (DPDPA):** - The Indian government has addressed the issue of data privacy in the digital age through the enactment of the Digital Personal Data Protection Act, 2023 (also known as DPDP Act or DPDPA-2023). It is an act of the Parliament of India to provide for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto.

- **FEATURES OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023:** -

The key features of the Digital Personal Data Protection Act, 2023 in India include:

- i. **Definition of Personal Data:** - The Digital Personal Data Protection Act, 2023 defines personal data as any data about an individual that can directly or indirectly identify that individual. This definition encompasses a broad range of information, whether stored electronically or in physical form, that can be used to identify a person. Personal data includes not only obvious identifiers like names and addresses but also more nuanced



data such as IP addresses, browser cookies, behavioural patterns, and other details that can be linked to an individual.

- ii. **Consent Requirement:** - Organizations are mandated to obtain clear, informed, and explicit consent from individuals before collecting, processing, or sharing their data. This emphasizes the importance of individual consent and transparency in data processing.
- iii. **Data Minimization Principle:** - The Act discourages the collection of unnecessary data, promoting the principle of data minimization. Organizations are required to collect only data relevant to their specified purpose, encouraging efficient data management practices.
- iv. **Right to Access and Rectification:** - Individuals have the right to access their data held by organizations, ensuring transparency in data processing. Additionally, individuals can request corrections to their data, empowering them to maintain accurate personal information.
- v. **Accountability and Transparency:** - The Act aims to hold organizations accountable for the data they collect and process, emphasizing transparency in data usage and providing recourse in case of violations. This ensures responsible data handling practices.
- vi. **Right to Erasure:** - Individuals have the right to request the deletion or erasure of their personal data under certain circumstances, giving them control over their information.
- vii. **Right to Restrict Processing:** - Individuals can request restrictions on the processing of their personal data by organizations, providing them with a level of control over how their data is used.
- viii. **Right to Object:** - Individuals can object to the processing of their personal data by organizations under specific conditions, allowing them to challenge data processing activities that they believe are not lawful or fair.
- ix. **Data Protection Officer (DPO):** - To ensure adherence to the act, organizations, especially those dealing with vast amounts of personal data, are required to appoint a Data Protection Officer. The DPO acts as the torchbearer for data protection within the organization, ensuring compliance, addressing concerns & acting as a bridge between the organization and regulatory authorities.

These features collectively establish a robust legal framework to protect personal data, empower individuals with rights over their data, and promote accountability and transparency in data processing practices in the digital age in India.

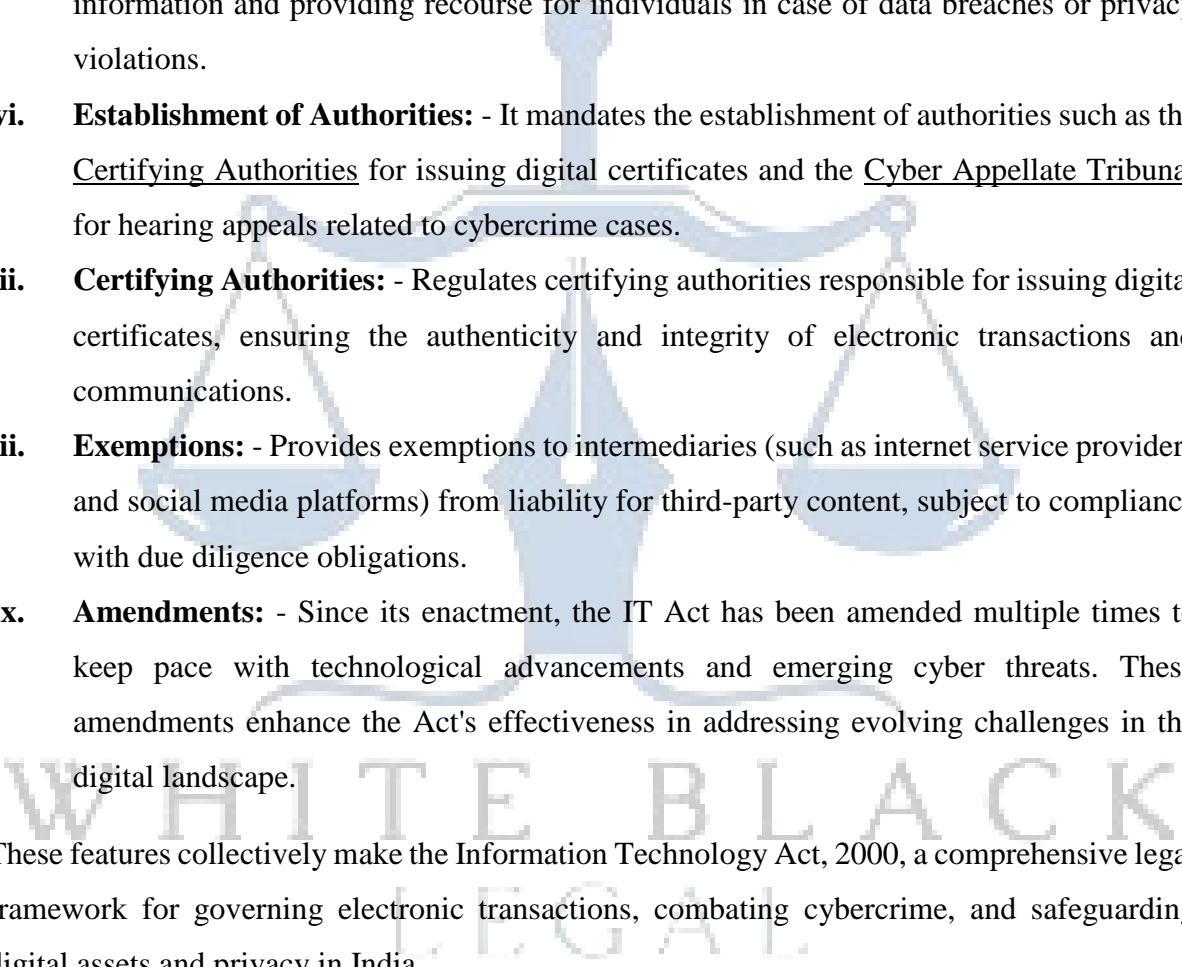
**2. Information Technology Act, 2000 (IT Act):** - The IT Act, along with the Information Technology (Amendment) Act, 2008, sets limits on processing personal information and imposes penalties for non-compliance with data protection obligations. The key provisions of the Information Technology Act, 2000 in India related to data protection include: -

- a) **Section 43A:** - This section holds corporate bodies accountable for negligence in implementing and maintaining reasonable security practices and procedures for sensitive personal data or information. If a body corporate fails to adhere to these security measures, leading to a breach of sensitive information, they are liable to pay damages as compensation to the affected individuals. This provision ensures that entities handling sensitive data are legally obligated to safeguard it, emphasizing the importance of maintaining adequate security controls to protect personal information from unauthorized access or disclosure.
- b) **Section 69:** - This provision is related to interception, monitoring, and decryption of information in India. It outlines that the Central Government, State Government, or authorized officers can direct agencies to intercept, monitor, or decrypt information in certain circumstances, such as for national security or public order reasons. The procedure and safeguards for such actions are to be prescribed, and those in charge of computer resources must provide technical assistance as required. Failure to comply can result in imprisonment and fines.
- c) **Section 72A:** - It penalizes the unauthorized disclosure of personal information by individuals or intermediaries. It suggests that anyone who discloses personal information without consent or in violation of a lawful contract may be subject to penalties of up to twenty-five lakh rupees.

- **Features of Information Technology Act, 2000:** -

The Information Technology Act, 2000 (IT Act) is a pivotal piece of legislation in India addressing various aspects of electronic commerce and cybercrime. The key features are: -

- i. **Legal Recognition:** - It provides legal recognition to electronic records and digital signatures, thereby facilitating electronic transactions and filing of documents with government agencies.
- ii. **Cybercrime Provisions:** - It defines offenses such as hacking, data theft, identity theft, and online fraud, along with corresponding penalties. It criminalizes unauthorized access to computer systems and networks.

- 
- iii. **Electronic Governance:** - It facilitates the use of electronic means for communication, filing, and storage of documents with government agencies, promoting e-governance initiatives.
  - iv. **Interception and Monitoring:** - The Act grants the government the power to intercept and monitor electronic communications under certain circumstances, primarily for national security reasons or in the interest of public safety.
  - v. **Data Protection and Privacy:** - It includes provisions for the protection of personal data and privacy in the digital domain, outlining responsibilities for entities handling sensitive information and providing recourse for individuals in case of data breaches or privacy violations.
  - vi. **Establishment of Authorities:** - It mandates the establishment of authorities such as the Certifying Authorities for issuing digital certificates and the Cyber Appellate Tribunal for hearing appeals related to cybercrime cases.
  - vii. **Certifying Authorities:** - Regulates certifying authorities responsible for issuing digital certificates, ensuring the authenticity and integrity of electronic transactions and communications.
  - viii. **Exemptions:** - Provides exemptions to intermediaries (such as internet service providers and social media platforms) from liability for third-party content, subject to compliance with due diligence obligations.
  - ix. **Amendments:** - Since its enactment, the IT Act has been amended multiple times to keep pace with technological advancements and emerging cyber threats. These amendments enhance the Act's effectiveness in addressing evolving challenges in the digital landscape.

These features collectively make the Information Technology Act, 2000, a comprehensive legal framework for governing electronic transactions, combating cybercrime, and safeguarding digital assets and privacy in India.

- 3. **Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011:** - The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, established guidelines for data protection in India. It mandates entities collecting sensitive personal data to implement reasonable security practices to safeguard information. These rules apply to organizations handling sensitive personal data such as passwords, financial

information, health records, etc. They outline measures like encryption, secure storage, and regular audits to ensure compliance. Non-compliance can lead to penalties. The rules aim to protect individuals' privacy and prevent unauthorized access, disclosure, or misuse of sensitive personal information in the digital age.

- 4. Sector-Specific Regulations:** - Regulators in India, such as the Reserve Bank of India (RBI) and the Insurance Regulatory and Development Authority of India (IRDAI), enforce sector-specific regulations that compel entities within their purview to adhere to cybersecurity standards. These standards are designed to safeguard sensitive data, financial transactions, and customer information from cyber threats. Institutions operating in sectors like banking, insurance, and finance are required to implement robust cybersecurity measures to ensure compliance with regulatory directives. Failure to meet these standards can result in penalties, reputational damage, and legal consequences, underscoring the importance of cybersecurity in the digital age.

## **GLOBAL PERSPECTIVE OF REGULATING DATA PROTECTION AND PRIVACY**

Data protection and privacy are fundamental in safeguarding personal information, ensuring it's collected, processed, and stored securely and ethically. Compliance with regulations like GDPR and CCPA is vital, as they dictate how data should be handled, minimizing the risk of misuse or unauthorized access. Implementing robust security measures, such as encryption and access controls, helps prevent data breaches and maintains individuals' trust. Privacy-enhancing technologies and transparent policies further support data protection efforts, fostering a culture of accountability and respect for privacy rights in the digital landscape.

- **European Union:** - The European Union, particularly with the implementation of the **General Data Protection Regulation (GDPR)**<sup>1</sup> in **2018**, is recognized for having some of the most stringent data protection and privacy laws globally. The General Data Protection Regulation (GDPR) is a comprehensive data protection and privacy regulation established by the European Union (EU) in 2018. It applies to organizations worldwide that process the personal data of EU citizens or residents, or offer goods or services to such individuals. The GDPR aims to protect individuals' privacy rights and enhance data security, with provisions covering territorial scope, definitions, data controller obligations, consent requirements, data subject rights, and penalties for non-compliance. Violations can result in fines of up to **€20 million or 4% of global revenue, whichever is higher**, and data subjects have the

---

<sup>1</sup> WIKIPEDIA, [https://en.m.wikipedia.org/wiki/General\\_Data\\_Protection\\_Regulation](https://en.m.wikipedia.org/wiki/General_Data_Protection_Regulation) (last visited Apr. 8, 2024).



right to seek compensation for damages. The GDPR is known for its stringent requirements and significant penalties, making it a crucial consideration for organizations operating in the EU or handling EU citizens' data.

▪ **COMPARISON BETWEEN INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT AND EUROPEAN UNION'S GDPR: -**

- i. Applicability:** - The GDPR applies to any organization, regardless of its location, that processes personal data of individuals located in the European Union (EU). This means that even if a company is based outside the EU, if it handles the personal data of EU residents, it must comply with the GDPR. On the other hand, the DPDPA applies to organizations processing personal data of individuals located in India, irrespective of the organization's location. This difference in applicability means that businesses operating in either the EU or India need to ensure compliance with the respective laws based on the location of the individuals whose data they process.
- ii. Consent:** - Under the GDPR, obtaining consent for processing personal data is a stringent requirement. Consent must be freely given, specific, informed, and unambiguous, and individuals must have the option to withdraw consent easily. Consent mechanisms must be clear and transparent, ensuring that individuals understand what they are consenting to. While the DPDPA likely has similar consent requirements, there may be variations in how consent is obtained and managed, depending on the specific provisions of the Indian law and its interpretation by regulatory authorities.
- iii. Data Transfer Rules:** - The GDPR imposes strict rules on the transfer of personal data outside the EU to ensure adequate protection of individuals' rights and freedoms. Organizations must implement appropriate safeguards, such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs), when transferring data to countries without an adequacy decision from the European Commission. Conversely, the DPDPA likely has less stringent requirements for cross-border data transfers, which may facilitate easier data flows outside of India. This distinction in data transfer rules reflects differing approaches to international data transfers between the EU and India.
- iv. Purpose and Goals:** - The GDPR aims to empower individuals by giving them control over their personal data, simplify the regulatory landscape for businesses operating

internationally, and enhance the protection of personal data from unauthorized processing. It is designed to harmonize data protection laws across the EU member states and strengthen individuals' rights concerning their personal data. On the other hand, the DPDPA seeks to protect the privacy of Indian citizens' personal data, promote responsible use of personal data, empower individuals to exercise control over their data, and foster innovation and economic growth within India. While both laws share the overarching goal of protecting personal data, they reflect different cultural, legal, and economic contexts.

- v. **Enforcement Mechanisms:** - The GDPR grants enforcement powers to Data Protection Authorities (DPAs) in each EU member state, empowering them to investigate complaints, conduct audits, and impose fines and penalties for violations of the regulation. DPAs play a crucial role in ensuring compliance and enforcing the GDPR's provisions, thereby contributing to the consistent application of data protection rules across the EU. While the enforcement mechanisms of the DPDPA are not explicitly outlined, it is likely that Indian regulatory authorities will have similar powers to investigate non-compliance and impose sanctions on organizations that violate the law.
- vi. **Penalties for Non-Compliance:** - The GDPR introduces substantial penalties for non-compliance, with fines of up to €20 million or 4% of the organization's global annual turnover, whichever is higher, for serious violations. These penalties serve as a deterrent and incentivize organizations to prioritize data protection and compliance efforts. While specific penalties under the DPDPA are not detailed, it is expected that non-compliance will result in fines and other punitive measures, similar to those imposed under the GDPR. Effective enforcement of penalties is essential for ensuring accountability and promoting a culture of data protection compliance among organizations operating in India.

- **Lessons learned from the comparison of India's Digital Personal Data Protection Act and European Union's GDPR:** -

After analysing the comparison between India's Digital Personal Data Protection Act (DPDPA) and the European Union's General Data Protection Regulation (GDPR), some changes that could be considered for the DPDPA include: -

- i. **Operational Impacts:** - The DPDPA could benefit from incorporating operational impacts similar to the GDPR, such as direct obligations on data processors, clear guidelines on

contractual protections passed on to data processors, and specific requirements for consent managers to ensure accountability and data sharing practices.

- ii. Data Subject Rights:** - Enhancing data subject rights under the DPDPA to align more closely with the GDPR could involve providing data principals with additional rights, such as the right to compensation in case of non-compliance, and clarifying the threshold for what constitutes a “significant” breach to ensure consistency and transparency.
- iii. Cross-Border Data Transfers:** - The DPDPA could consider revising its approach to cross-border data transfers to provide more clarity and guidance on international data transfers, including mechanisms for ensuring data protection when personal data is transferred outside of India.
- iv. Data Breach Notification:** - Introducing specific deadlines for reporting data breaches under the DPDPA could enhance transparency and accountability, ensuring that data fiduciaries promptly notify the Data Protection Board and affected individuals of any breaches, regardless of their magnitude or risk of harm.
- v. Significant Data Fiduciaries:** - The DPDPA could further define the criteria for classifying significant data fiduciaries, specifying the obligations and responsibilities of these entities, including the appointment of independent auditors and conducting data protection impact assessments to ensure compliance and accountability.

By incorporating these changes, the DPDPA could strengthen its data protection framework, enhance data subject rights, improve transparency and accountability in data processing practices, and align more closely with global data protection standards, such as those set by the GDPR.

WHITE BLACK  
LEGAL