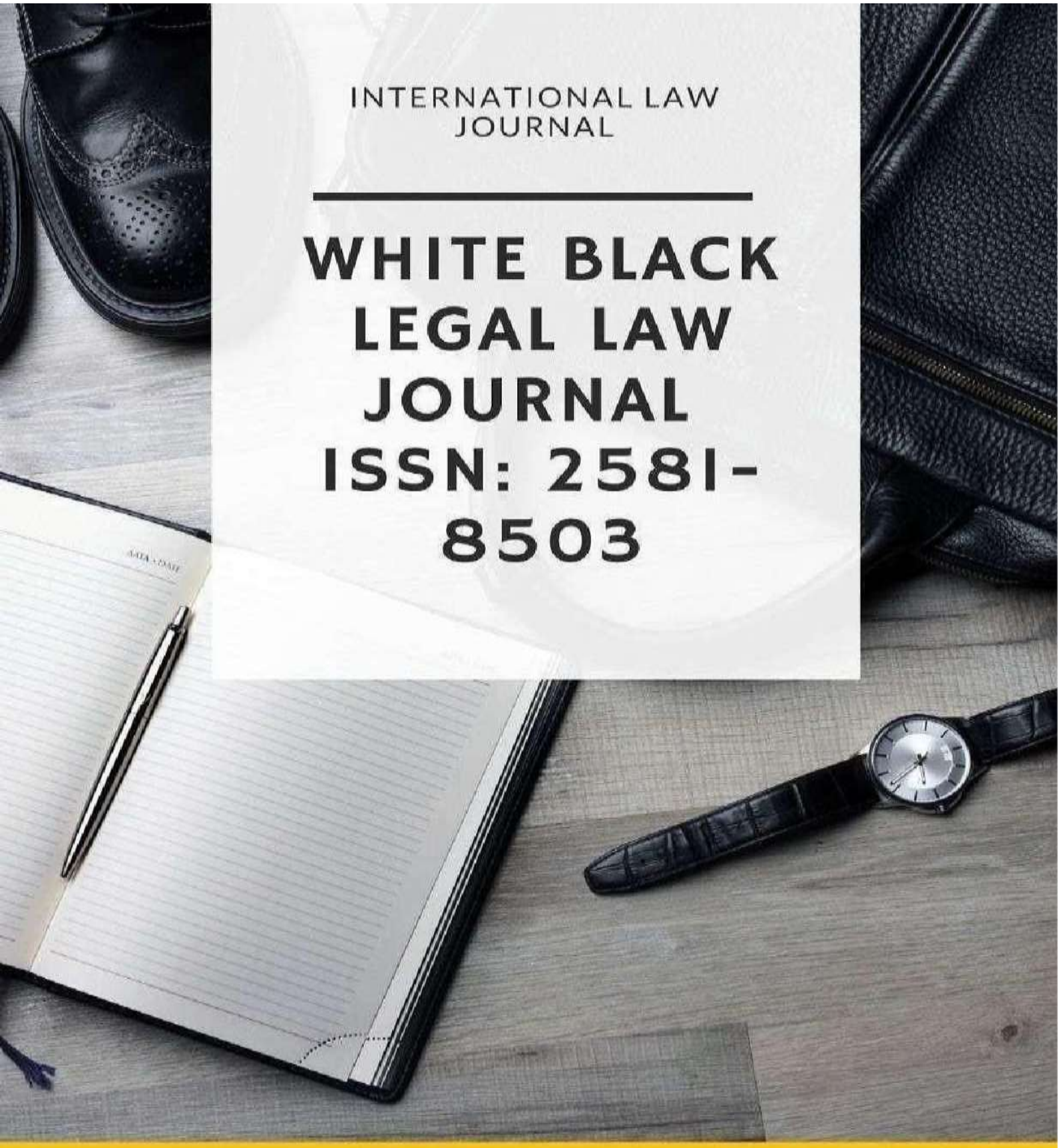

INTERNATIONAL LAW JOURNAL

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

DISCLAIMER

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 a professional diploma in Public 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

www.whiteblacklegal.co.in
Volume 3 Issue 1 | March 2025 ISSN: 2581-8503

THE DATA PROTECTION ACT 2023: ITS IMPACT ON BUSINESSES, COMPLIANCE STEPS, AND PENALTIES FOR VIOLATIONS

AUTHORED BY - SIMRAN AGARWAL

The significance of **data privacy** has grown along with the growth in Internet usage over time. Social media platforms, apps, and websites frequently need to gather and keep user's personal information to function. However, some platforms and apps might collect and use data more than users had anticipated, giving them less privacy than they had anticipated. The privacy of users may be jeopardized by a data breach caused by other apps and platforms that do not adequately protect the data they gather. In general, data privacy refers to an individual's autonomy over the decision of when, how, and to what degree personal information about them is disclosed to third parties. This personal data may include a person's name, address, phone number, online or offline behavior, or any data related to personal information. Notably, it may be the case that someone may want to keep others out of private information thereby warranting the need for data protection laws.[1]

What is Data Protection?

Data Protection, which is frequently used interchangeably with "data security" refers to the methodical and strategic actions taken to ensure the confidentiality, accessibility, and integrity of sensitive data. These safeguards, which are essential for businesses that gather, handle, or keep private information are meant to stop data loss, damage, theft, or corruption. A strong data protection plan mechanism is essential at a time when data generation and storage are growing at a never-before-seen rate. In order to maintain trust and compliance in data-centric operations, the main objective of data protection is not only to protect sensitive information but also to make sure that it is dependable and accessible.

Why is Data Privacy so crucial?

Data privacy is essential for several reasons, such as protection from fraud and identity theft, discrimination, manipulation and exploitation, and so on. In terms of organization data privacy

[1] Atlan, Data Privacy - Definition, Importance and examples, 12 December 2023

is crucial:-

i) Developing Reputation and Trust - Safeguarding consumer data enhances user and customer relationships and fosters trust, both of which are essential for company success.

ii) Ensuring Legal Compliance - Organisations that violate the stringent data protection laws implemented by numerous nations and regions risk severe penalties.

iii) Lowering the Risk of Data Breaches - Robust data privacy procedures can aid in lowering the risk of data breaches, which may result in monetary losses, harm to one's reputation, and legal repercussions.

iv) Competitive Advantage - Businesses that put data privacy first can differentiate themselves from rivals by showcasing their dedication to safeguarding client information.

v) Ethical Obligation - Companies have an ethical obligation to safeguard client information and make sure it is managed sensibly and openly.[2]

Up until 2023, India lacked a separate data protection framework or law.The Information Technology Act of 2000 (IT Act) and its notified regulations served as the cornerstone of the data protection framework. The 2011 Information Technology Privacy Rules (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) were one of these. A nine-judge constitutional bench of the Indian Supreme Court ruled in Justice K. S Puttaswamy v. Union of India maintained that the right to privacy is a fundamental right, enshrined in Article 21 (Right to Life and Liberty) of the Indian Constitution. Consequently, a comprehensive framework for data protection was created for India. After releasing multiple draft versions of a data protection law and considering the recommendations from numerous stakeholders, the Ministry of Electronics and Information Technology (MeitY), Government of India, released the Digital Personal Data Protection Bill in 2022 (DPDP Bill).[3]

The final draft of the DPDP Bill, which was accepted by both houses of the Indian Parliament, included a few significant changes from the original. The Indian government unveiled the Digital Personal Data Protection Act, 2023 (DPDP Act) on August 11, 2023, which will act as the country's legal framework for protecting personal data. The Indian government has released a draft of the regulations pertaining to the DPDP Act; however, the provisions of the Act have not yet been implemented.

[2] Pecb, Data Protection - Definition and Importance, 10 November 2021
[3] CookieYes, Guide to India's Digital Personal Data Protection Act,7 January 2025

IT ACT, 2000, And Digital Personal Data Protection Act, 2023

The IT Act does not offer a thorough framework for data privacy, but it does cover a wide range of electronic activities, including data protection. The DPDP Act is a data protection law that provides a contemporary, all-inclusive privacy framework and data governance for the digital era. Before processing personal data, the act expressly requires individual's informed, specific, and explicit consent. The IT Act provides limited individual rights whereas the DPDP Act gives people several rights, such as the ability to view, amend, and remove their personal information. Although the IT Act established the framework for dealing with cybercrimes and safeguarding sensitive information, the DPDP Act is a much-needed revision meant to safeguard personal information in contemporary, digitally-first society. The IT Act, 2000 was created to address cybercrimes, give legal recognition to digital signatures, and facilitate electronic transactions. However, the Digital Personal Protection Data Act, 2023 was created because the IT Act was not specifically created to address the extensive and contemporary complexities of personal data protection and privacy.[4]

Digital Protection Laws

Businesses need to review their data management plans in light of the Data Protection Law of 2023. They must ensure compliance by implementing measures that address consent, data accuracy, secure processing, and the prompt deletion of personal data after its goal has been achieved.

The provisions of the Data Protection Act are designed to ensure the protection of personal data and safeguard the privacy of individuals. Businesses also referred to as Data Fiduciaries, must comply with these provisions to maintain transparency, accountability, and security in their data processing activities. The implementation of these provisions can have a significant impact on how businesses handle data, and it will require them to adopt specific measures to comply with the law.

Here's a breakdown of the key provisions of the Data Protection Act, the impact they will have on businesses, and the measures businesses will need to take to ensure compliance:

[4] Law.aisa, The key aspects of India's Data Protection Act, 18 April 2024

1) Section 4 of the act states the grounds for processing personal data. Businesses must confirm that they are processing personal data for lawful purposes, either based on consent from an individual or for other legitimate purposes as defined by law.
2) Section 4(1)(a) of the act states that consent must be explicitly obtained from the data principal (individual). This could involve creating clear and understandable consent forms or mechanisms for individuals to provide their consent.
3) The consent request should clearly explain the purpose of data collection, ensuring that it complies with the lawful provision of the act.
4) According to section 5(1) of the act, every consent request made to the data principal must be accompanied by a notice providing the following information :

   i) The notice should clearly communicate what personal data is being collected and for what purpose.

   ii) The notice should inform the data principal about their rights, including the right to withdraw consent and how to exercise their rights.
5) Businesses must set up a system to allow data principals to exercise their rights, including withdrawing consent, accessing personal data, correcting, requesting, and deletion of data. The notice must explain these rights and provide easy methods for data principals to act on them. The notice must be specific and as per the compliance format.
6) Businesses that process data must ensure they handle personal data responsibly and in compliance with the relevant data protection law.
7) They need to update or implement their data protection policies, systems, and procedures to comply with the law.
8) In a case where a Data Principal has already given consent for processing their personal data before the commencement of the Act. Then the entity responsible for processing the data is required to take specific actions to ensure compliance with the new data protection law.
9) The business will need to ensure that its existing privacy notices are updated to reflect the new legal requirements, even for the data processed before the commencement of the act. It should include clear instructions on how to exercise rights under the new law and provide details on how to make complaints.
10) Businesses must deliver the notice to the data principal in a manner appropriate (eg., via email, postal mail, or through an online portal depending on how the original consent was obtained.
11) The notice should be clear, concise and accessible to the data principal.

12) Businesses should ensure that they keep records of when and how the notice was provided to the data principal, as the documents may be required for compliance purposes.
13) Businesses must provide notice in a language that is understood by the data principal and ensure that consent can be withdrawn easily.
14) As per section 9 of the act before processing any personal data of a child or a person with a disability who has a lawful guardian, businesses (data fiduciaries) must obtain verifiable consent from the child or person with a disability.
15) Businesses must ensure the consent is verifiable. This could involve methods such as email confirmation, phone verification, or using a third-party service to verify consent.
16) Data Fiduciaries must not engage in any data processing that could have a detrimental effect on the well-being of a child. This means businesses should avoid practices that could harm a child either physically, psychologically, or socially.
17) As per section 9 (3) of the act states that businesses are prohibited from engaging in tracking or behavioral monitoring of children and from carrying out targeted advertising directed at children.
18) The provisions in section 9(1) and section 9 (3) may not apply to certain classes of data fiduciaries or specific purposes, provided these are prescribed by the government.
19) Section 9(5) of the act talks about the exemption based on safe processing. The central government may allow certain data fiduciaries to be exempt from some of these obligations if they can demonstrate that their processing of children's data is done in a verifiably safe manner.
20) Section 12(2) of the act talks about the right to correction, completion, and updating of data which businesses must take action upon receiving a request from a data principal to correct, complete, or update their personal data.
21) Section 122(3) of the act talks about the right to erasure of personal data. A data principal has the right to request the erasure of their personal data, and businesses must comply with the request unless retention of data is necessary and is in compliance with the law.
22) The manner in which a data principal makes a request for erasure, and possibly for correction and updating, will be prescribed by the relevant regulatory authority or government. Businesses will need to adhere to these prescribed methods.[5]

[5] Meity.gov.in, The Digital Personal Data Protection Act,2023, 11 August 2023

23) Failure to comply with the provisions of the Act will result in the imposition of **penalties**.

Sl.No.	Breach of Provisions	Penalty
1.	Breach in observing the obligation of data fiduciary to take reasonable security safeguards to prevent a personal data breach under section 8(5)	May extend to two hundred and fifty crore rupees
2.	Breach in observing the obligation to give the board or affected data principal notice of a personal data breach under section 6 (8)	May extend to two hundred crore rupees
3.	Breach in observance of additional obligations in relation to children under section 9	May extend to two hundred crore rupees
4.	Breach in observance of additional obligations of significant data fiduciary under section 10	May extend to one hundred and fifty crore rupees
5.	A breach in observance of the duties under section 15	May extend to ten thousand rupees
6.	Breach of any other provisions of this Act or the rules made thereunder	May extend to fifty crore rupees

The DPDPA 2023 has had a profound impact on a wide range of business sectors, changing how operations are carried out in the following areas:

Financial Services: Since data is essential to processes like credit scoring, risk assessment, and fraud detection, financial institutions are now required to obtain express consent before processing data. Long-term relationships are maintained through the Act's promotion of transparency and strengthening of customer trust, despite the possibility that compliance will result in higher operating costs.

E-commerce: Processing children's data is one of the major issues that e-commerce companies must deal with. Nowadays, parental approval is needed for child-targeted advertising and profiling. In order to comply with the new regulations, businesses must adopt "privacy by design," implement privacy frameworks and modify their marketing strategies.

Healthcare: When collecting or sharing patients' sensitive medical data, the healthcare industry must get their express consent. This mandate is driving investments in safe data processing and storage technologies to safeguard vital health data.

Technology and IT Services: Organizations that handle a lot of user data are reevaluating their data management systems. To maintain compliance, handle data breaches, and defend user rights, they are implementing cutting-edge privacy technologies—incorporating data protection into the innovation lifecycle.[6]

Conclusion

In conclusion, the Digital Personal Data Protection Act 2023 marks the beginning of a new era for Indian companies. The Act promotes confidence in the digital economy by placing a high priority on accountability, transparency, and customer empowerment. As companies adjust to these developments, they ought to see compliance as a driving force behind creativity and long-term expansion. In this changing environment, companies that align their operations with the DPDPA will not only comply with legal requirements but also establish a strong basis for sustained success in a world that is driven by data.

Possibilities Amid Difficulties Although the DPDPA necessitates investment, it also offers chances for creativity and fostering trust. Companies that actively welcome these developments can establish themselves as industry leaders in data security and ethics. The Act also encourages privacy-focused innovation, including next-generation consent procedures, anonymized processing, and secure data analytics. Businesses can use data protection as a competitive advantage in an increasingly digital economy by making it a top priority.[7]

[6] Jisasoftech, Impact of Digital Personal Data Protection Act 2023 on Businesses in India, 21 February 2025
[7] Usercentrics, India Digital Personal Protection Act Overview, 21 February 2024