The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

DATA PRIVACY AND CYBERSECURITY: LEGAL IMPLICATION FOR BUSINESS

~ Anshika Jain

ABSTRACT

This article covers the increasing significance of data privacy and cyber security in today's business landscape and discusses the legal considerations that come into play when businesses collect, process, store and protect personal data. It asserts that data is not just operational information anymore but a valuable asset for business and at the same time can be a point of legal risk if it is mishandled, exposed or processed without proper security measures. The article highlights the Indian laws, including the Digital Personal Data Protection Act, 2023, Information Technology Act, 2000, and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, to illustrate the new obligations on businesses regarding consent, security measures, notification of data breaches, children's data and accountability. It also examines the potential for regulatory penalties, claims for compensation, reputational damage and heightened regulatory attention to managerial and board-level oversight in the event of an incident or breach in the cyber realm. The article also notes on the compliance burden in sectors, practical challenges faced by Indian businesses, the importance of privacy by design, training, technical protection, audit program and better vendor management. It finds that data privacy and cybersecurity are now integral parts of legal governance and business survival and that businesses in India need to put in place more systematic and proactive compliance regimes to be able to do business responsibly in the digital economy.

INTRODUCTION

The Data of any company in current times are like their jewels which need to be secure at any cost but due to the expansion of cyberspace in the field of cybercrimes which is equal to the expansion in the development of technology. As technology advances, crime also increases,

particularly crimes related to data breaches involving confidential and sensitive information. It becomes must for the business to secure their data. Data privacy means managing how personal data is collected, used, meanwhile cybersecurity simply means protection of data from the hackers, breach and misuse. This topic is a crucial part for any businesses because they deal with customer data, website data, employee data, company's confidential data on every day basis. Hence legal implications are enforced on every business activity.[1]

DATA AS A BUSINESS ASSET AND SOURCE OF LEGAL RISK

The meaning of data is not bound to collection of information anymore, it has become a business asset similar to money, land or machinery. Business uses data-driven decision-making (DDDM) approach which focuses on analysis of data such as customer, feedback, market trends and financial data for making informed business decision.[2] Those decisions can be related to targeted marketing campaigns and update its recommendation engine, since in modern times the marketing is solely relied on algorithm which feeds on data. Mishandling of those data can lead to breach of customer trust, legal penalties and fines. There are broadly three types of data misuse by businesses. The first is commingling, which occurs when a business collects data for a specific purpose but subsequently uses it for a different purpose without obtaining the customer's consent. The second is personal benefit, where a business uses customers' data for its own personal or commercial advantage rather than for the purpose for which it was collected. The third is ambiguity, which arises when a business fails to clearly specify the purpose for collecting and processing personal data. Such forms of data misuse can expose businesses to significant legal risks, including financial losses, reputational damage, and operational disruptions resulting from lawsuits, regulatory penalties, or unenforceable contracts.

.

INDIAN LEGAL FRAMEWORK ON DATA PRIVACY AND CYBERSECURITY

The Indian legal framework governing data privacy and cybersecurity primarily comprises the Digital Personal Data Protection Act, 2023 (DPDP Act**)** and the Information Technology Act, 2000 (IT Act**)**. These laws establish the legal framework for the collection, processing,

[1] DLA PIPER, *Data Protection Laws of the World: India*, https://www.dlapiperdataprotection.com/?t=law&c=IN (last visited May 20, 2026).
[2] IBM, *What Is Data-Driven Decision-Making (DDDM)?*, https://www.ibm.com/think/topics/data-driven-decision-making. (last visited May 21, 2026).

protection, and security of personal data while addressing cyber-related offences and ensuring compliance with data protection requirements.

The Digital Personal Data Protection Act, 2023 mentions how personal data should be collected, processed and used, it put emphasis on the consent of the consumer regarding the use of their data and give data subject rights related to access, correction and deletion. It defines obligations for significant data fiduciaries, including appointing a Data Protection Officer (DPO). The act imposes penalties up to ₹250 Crore in case of non-compliance. The Information Technology Act, 2000 & IT (Reasonable Security Practices) Rules addresses Cybercrime Penalties, protection for personal data which is sensitive in nature and it also define guidelines for corporate security practices.

BUSINESS OBLIGATIONS UNDER PRIVACY AND CYBERSECURITY LAW

The businesses have certain obligations, they need to imply according to the Privacy and cybersecurity Law known as Digital Personal Data Protection Act, 2023.

Reasonable security safeguards: The business should implement reasonable safeguards such as data encryption, restrict access to personal data only to limited authority, maintain detailed audit logs regarding access and use of data, data backups should be maintained, update contracts with data processors to follow above safeguards.

Consent Notices: The consent notices should be easy to read, language should be understandable by the borrower, state the type and purpose of collected data, privacy centre should also be maintained.

Consent Exemption: The consent should be exempted when the data is collected for research purpose, the user voluntarily give the data, the data process by state for the purpose of emergencies, disaster response, public health or employment.

Notifications for breach: In case of breach of personal data the business should notify the Data Protection Board (DPB) within 72 hours, it should also notify Data Principals immediately regarding the breach, its impact, steps for mitigation.

Verify Parental Consent: If the user is under 18 years the business must obtain verifiable parental consent before processing their data.

CYBER INCIDENTS, LIABILITY, AND CORPORATE ACCOUNTABILITY

A cyber incident refers to any act or event that threatens or compromises the confidentiality, integrity, or availability of digital information. A data breach is a type of cyber incident in which confidential, sensitive, or personal information is accessed, stolen, disclosed, or exposed to unauthorized individuals.

Cyber incidents that result in data breaches can have serious legal consequences. Businesses are expected to protect the personal information they collect, process, and store. Failure to meet these obligations may result in regulatory action, financial penalties, contractual disputes, compensation claims, and a loss of customer trust. Therefore, the law treats a data breach not merely as a technical failure but as a significant legal issue that may attract civil and regulatory liability.[3]

The IT team will not be the only one who will be held liable in case of non-compliance the company's management will also be held accountable for weak compliance. The company's board and leaders are expected to make sure that there should be proper privacy policies, employee training, security controls and a clear plan in case of cyber incidents. Since the cyber risk affects the whole business not just computer the board level oversight also matters and if the leaders ignore it the company will be portrayed as careless which will lead to legal and reputational damage.

PRACTICAL BARRIERS TO IMPLEMENTATION IN INDIAN BUSINESSES

Practical barriers refer to the actual challenges encountered by businesses that prevent them from effectively complying with privacy and cybersecurity regulations. In India, awareness about the requirements of the law is still low on the team level, with many companies not fully understanding what the law requires. This is exacerbated in the absence of strong privacy training, as employees can click on untrustworthy links, share information recklessly, and miss internal guidelines. Budget constraints are also a factor, particularly for small and medium businesses, as privacy compliance takes time, software, trained personnel and constant monitoring.

Old systems and legacy IT is another big obstacle, those systems that are no longer supported or secure may not be able to accommodate modern privacy controls. A lot of companies also

[3]ICSI, *Data Privacy & Cybersecurity: A Governance Imperative* https://www.icsi.edu/media/webmodules/CSJ/March-2025/18.pdf (last visited May 15, 2025).

rely on a number of vendors, adding to the confusion of who's responsible for data security. Lack of communication between legal, IT and management teams can slow down decision making and hinder compliance. In the simpler terms, the law is clear, but businesses often find that the day-to-day implementation of the law is difficult because people, systems, money and communication are not working optimally.

COMPLIANCE STRATEGIES AND REGULATORY RECOMMENDATIONS

Adopt privacy by design, as privacy and cyber security should be embedded into systems from the outset, not tacked on afterwards. When a company builds a website, app, internal database or customer portal, it should consider what data is necessary, who should have access to it and how it will be safeguarded. In addition, data minimization should be adhered to – collecting only data that is actually required for the business purpose and discarding it when no longer needed. These two practices limit the exposure of data to the sensitive aspects and are also good for the business to demonstrate their responsible and legal practice.

Effective technical and organisational measures, such as encryption, masking, employee awareness training, auditing logs and breach response plans should also be implemented in addition. Employee training minimizes human error issues such as weak passwords, sharing, phishing attacks, etc., and use of encryption and masking protects data from misuse in the event of unauthorized access. The value of audit logs lies in the fact that they track access to data, its changes and who has access to it at what time, allowing for the rapid identification and investigation of issues. Last but not least, a business should have a clear breach response plan and have robust vendor contracts in place, so that if a cyber incident does occur, the company is able to respond quickly, identify the appropriate response party and safeguard the trust of their customers and legal compliance.

CONCLUSION

To sum up, the article demonstrates how data privacy and cybersecurity have emerged as key legal and business issues for any businesses conducting business in India, particularly given the significance of personal data in businesses for their day-to-day operations, customer engagements, and digital expansion. The conversation shows that it's not just a matter of meeting the standards, it's a matter of facing regulatory risk, business interruption, damage to reputation, and loss of customer trust. Indian enterprises are thus required to have robust privacy infrastructure, greater internal understanding, and more streamlined governance processes to address new commitments under the evolving data privacy landscape in India.

Going forward, privacy by design, enhanced security measures, improved employee training, increased management accountability, and a more sophisticated compliance culture built around data protection as an ongoing component of business and responsible corporate practice will become key components of future improvement.