WHITE PAPER ON

DATA PROTECTION COMPLIANCE FOR MSMES AND STARTUPS

under Digital Personal Data Protection Act 2023

Center for Innovation, Incubation & Legal Entrepreneurship, CNLU Patna

AND

LL.B Mania

MARCH 2025

About Chanakya National Law University

Chanakya National Law University was established under the Chanakya National Law University Act, 2006 (Bihar Act No. 24 of 2006) on July 15, 2006, with the altruistic goal of serving society by disseminating high-quality legal education and legal awareness. CNLU provides quality multidisciplinary education in legal studies, keeping in view the demands of the global economy on the one hand and the needs of the domestic society on the other hand. It organizes advanced studies and promotes research in all branches of law to promote cultural, legal and ethical values with a view to promote and foster the rule of law and the objectives enshrined in the Constitution of India.

About CIILE & Startup Cell

Centre for Innovation, Incubation, and Legal Entrepreneurship is a not-for-profit Centre at CNLU. CIILE encourages start-ups in the areas of Legal and Social Entrepreneurship within the institute and the society at large. The goal of CIILE is to motivate, build and promote out of box thinking, development of innovative ideas amongst start-ups. To build an environment that will facilitate the creation of social enterprise knowledge through research. CIILE also empower students to apply their entrepreneurship abilities to develop solutions for greater social impact through academia.

The Startup-Cell in CNLU was established by the Department of Industries, Govt of Bihar under the Bihar Startup Policy 2022. The objective of the Startup cell is to foster an entrepreneurship culture in the university and its surroundings. It focuses on mentoring, resources, and networking to help students transform innovative ideas into viable startups, promoting self-employment and innovation culture. Startup Cell has been ranked 3rd amongst all the startup cells of Bihar by Department of Industries, Bihar Government.

About LL.B Mania

LL.B Mania is Business Consulting Firm registered in MSME, Government of India (UAM No. JH-04-0001870) providing business strategy services, legal consulting and contract drafting services to early stage startups, startup founders. It also provides knowledge management services to Law Firms and Lawyers Chambers. LL.B Mania is also an incubatee under CIILE, CNLU Patna. LL.B Mania’s range of services extends to a myriad of professional solutions, including ghostwriting and copywriting services.

Contents

EXECUTIVE SUMMARY

The Digital Personal Data Protection Act (DPDPA), 2023 represents a significant milestone in India's journey toward robust data privacy regulation. With the increasing digitalization of services and the expansion of online business operations, concerns about data privacy, security, and the protection of individual rights have become more pressing. The DPDPA aims to address these challenges by creating a comprehensive legal framework that governs the collection, processing, and protection of personal data. This law is aligned with global data protection standards such as the General Data Protection Regulation (GDPR) of the European Union while incorporating provisions specific to India's socio-economic and technological landscape.

Startups and Micro, Small, and Medium Enterprises (MSMEs) must navigate this evolving regulatory framework carefully. While some provisions offer exemptions for smaller businesses, others impose stringent compliance measures, especially for companies handling sensitive data. Given that many startups operate on lean budgets and lack specialized legal expertise, understanding the nuances of the DPDPA is critical to avoiding penalties and ensuring smooth business operations.

The DPDPA applies to all entities processing personal data in digital form within India, as well as foreign businesses that offer goods or services to individuals in India. Data in non-digital form is not included in its purview.[1] The Act's broad scope ensures that businesses of all sizes, including MSMEs and startups, are brought under its regulatory purview.

Recognizing that compliance can be a significant burden for smaller organizations, the government has the authority to exempt certain categories of Data Fiduciaries, including startups and MSMEs, from specific obligations. The criteria for these exemptions depend on factors such as:

I. The volume of personal data processed by the business.
II. The sensitivity of the data collected, such as financial or health-related information.
III. The potential risk to individuals, including risks of identity theft, fraud, or privacy breaches.

While smaller startups processing limited data may receive some relaxations, those dealing with sensitive personal data or handling large-scale data operations may be designated as Significant Data Fiduciaries (SDFs) and subjected to additional compliance requirements. This classification is particularly relevant for fintech, healthcare, and e-commerce startups, which collect and process substantial amounts of personal and sensitive data.

[1] India's Digital Personal Data Protection Act, 2023: History in the Making, Nishith Desai, https://www.nishithdesai.com/NewsDetails/10703

KEY DEFINITIONS IN THE DIGITAL PERSONAL DATA PROTECTION ACT 2023

A. Data Fiduciary

A Data Fiduciary is any entity that determines the purpose and means of processing personal data. Businesses that collect user data, such as online marketplaces, social media platforms, or payment service providers, fall into this category. Data Fiduciaries are responsible for ensuring compliance with data processing principles, obtaining explicit and informed consent, and enabling user rights such as access, correction, and deletion of data.

B. Data Principal

The Data Principal refers to the individual whose data is being processed. Under the DPDPA, individuals have rights concerning their personal data, including:

i. The right to access information about how their data is used.

ii. The right to request corrections if their data is inaccurate.

iii. The right to request the deletion of their data when it is no longer necessary.

iv. The right to withdraw consent at any time.

For minors (below 18 years), parental consent is required, and businesses cannot engage in tracking, profiling, or targeted advertising toward children.

C. Significant Data Fiduciary (SDF)

An SDF is a special category of Data Fiduciary that processes large volumes of data or deals with high-risk sensitive data. The government determines which organizations qualify as SDFs based on:

i. The volume of data processed.

ii. The nature of personal data handled (e.g., financial, biometric, health records).

iii. The impact on national security or public welfare.

SDFs are required to conduct Data Protection Impact Assessments (DPIAs), undergo annual independent audits, and appoint a Data Protection Officer (DPO) to ensure compliance.[2]

D. Consent Managers

They are registered intermediaries under the DPDPA that enable Data Principals to give, manage, review, and withdraw consent in a transparent and accessible manner. They act as

[2] Guide to India's Digital Personal Data Protection Act (DPDP Act), CookieYes, https://www.cookieyes.com/blog/india-digital-personal-data-protection-act-dpdpa/

a bridge between Data Principals and Data Fiduciaries and are accountable for ensuring compliance with prescribed obligations.[3]

Personal Data vs. Sensitive Personal Data & Obligations

The DPDPA differentiates between personal data and sensitive personal data, each carrying different obligations for businesses.

A. Personal Data

Personal data includes any information that directly or indirectly identifies an individual, such as names, phone numbers, email addresses, or location data. The law mandates that organizations:

i. *Obtain clear and informed consent before processing such data.*

ii. *Provide mechanisms for individuals to correct or delete their data.*

iii. *Ensure basic security safeguards to protect data from breaches.*

B. Sensitive Personal Data (SPD)

While the DPDPA does not explicitly define Sensitive Personal Data (SPD), the government has the authority to classify certain data categories as sensitive. Likely examples include:

i. *Financial information, such as credit scores and banking details.*

ii. *Biometric and genetic data, including fingerprints and DNA information.*

iii. *Health records, such as medical histories and prescription details.*

iv. *Religious and political affiliations.*[4]

Businesses handling SPD must implement higher security standards, including encryption, explicit consent requirements, and additional restrictions on cross-border data transfers.

[3] Consent Manager under Digital Personal Data Protection Act 2023: A Unique Approach to Data Privacy, Bar and Bench, https://www.barandbench.com/law-firms/view-point/consent-manager-under-digital-personal-data-protection-act-2023-a-unique-approach-to-data-privacy

[4] Sense and Sensitivity : 'Sensitive' Information Under India's New Data Regime, S & R Associates, https://www.snrlaw.in/sense-and-sensitivity-sensitive-information-under-indias-new-data-regime/

PENALTIES & ENFORCEMENT MECHANISMS

The Data Protection Board of India (DPBI) serves as the primary regulatory authority overseeing compliance. The DPBI has the power to investigate complaints, monitor adherence to the Act, and impose penalties for violations.

Penalties for Non-Compliance

The DPDPA imposes strict penalties for businesses that fail to comply with its provisions. Key violations and their corresponding fines include:

Sr. No.	Violation	Penalty
1.	Breach of security safeguards	Up to INR 250,00,00,000 (two fifty crores)
2.	Failure to notify the Board or affected data principal of a breach	Up to INR 200,00,00,000 (two hundred crores)
3.	Breach of obligations concerning children	Up to INR 200,00,00,000 (two hundred crores)
4.	Breach of obligations for significant data fiduciaries	Up to INR 150,00,00,000 (one fifty crores)
5.	Breach of duties of data principal	Up to INR 10,000
6.	Breach of voluntary undertakings accepted by the Board	Penalties vary based on the breach
7.	Any other violations of the DPDPA or its rules	Up to INR 50,00,00,000 (fifty crores)

Beyond financial penalties, businesses that repeatedly violate data protection laws may face legal action, reputational damage, and loss of consumer trust.[5]

[5] Digital Personal Data Protection Act Edition VIII, JSA Advocates & Solicitors, https://www.jsalaw.com/wp-content/uploads/2024/11/DPDPA-Prism-Enforcement-and-penalties_Edition-8_Final.pdf

COMPLIANCE CHALLENGES FOR MSMEs UNDER THE DPDPA

The Digital Personal Data Protection Act (DPDPA) mandates strict data protection compliance, posing significant challenges for Micro, Small, and Medium Enterprises (MSMEs) due to their limited financial, legal, and technological resources. While MSMEs rely on digital platforms, cloud storage, and third-party services to stay competitive; compliance with DPDPA presents hurdles in terms of costs, awareness, vendor risks, and cross-border data restrictions. The following sections outline the key challenges MSMEs may face under the DPDPA and their implications.

1. Limited Resources: Legal Expertise & IT Infrastructure

A major challenge for MSMEs in DPDPA compliance is their limited financial, legal, and technological resources. Unlike large corporations with dedicated compliance teams, MSMEs operate with small teams where data protection is not a primary focus.[6]

i. Legal and Compliance Burdens

DPDPA compliance requires MSMEs to (i) implement consent mechanisms, (ii) data minimization, (iii) risk assessments, and (iv) audits, often necessitating legal experts, compliance documentation, and staff training. Without in-house legal teams, MSMEs rely on costly external consultants, and lacking proper policies may risk regulatory penalties.

ii. Technology and IT Infrastructure Gaps

MSMEs face challenges in technological readiness, often relying on outdated systems lacking strong security protocols. DPDPA mandates encryption, secure storage, and breach response mechanisms, requiring financial investment and technical expertise[7]—both scarce in MSMEs. Compliance demands trade-offs with business expansion, product development, and marketing.

2. Lack of Awareness About Data Processing Obligations

A major challenge for MSMEs is a lack of awareness about data privacy regulations. Without dedicated compliance teams, they often misunderstand their data protection responsibilities.[8]

---

[6] Namita Viswanath & Raghav Muthanna, "Top 6 Operational Impacts of India's DPDPA- Enforcement and the Data Protection Board (October 2023), available at: https://induslaw.com/publications/pdf/alerts-2024/top-six-operational-impacts-of-india%E2%80%99s-dpdpa-enforcement-and-the-data-protection-board.pdf (last accessed 16 March 2025).

[7] "Navigating Data Breach Compliance: A Guide for Startups under the DPDP Act", T&R Law Offices (January 4 2025), available at: https://tandrlawoffices.in/navigating-data-breach-compliance-a-guide-for-startups-under-the-dpdp-act/ (last accessed 16 March 2025).

[8] Shivangi Mishra, "Impact of Digital Personal Data Protection Act 2023 on MSMEs" (March 5 2025), available at: https://amlegals.com/impact-of-digital-personal-data-protection-act-2023-on-msmes/# (last accessed 16 March 2025).

i. Challenges in Understanding Data Processing Responsibilities

MSMEs struggle with identifying personal data, consent requirements, storage limits, and their role under DPDPA. Many unknowingly mishandle data, risking violations and legal liabilities, as Data Principals can file complaints for non-compliance.

ii. Lack of Awareness Leading to Non-Compliance Risks

Without guidance, MSMEs may collect data without consent, lack transparency, deny Data Principals' rights, or fail to maintain records, risking audits, consumer complaints, and fines. Digital MSMEs face heightened exposure, worsened by lack of government-led training.

3. Vendor & Third-Party Risks in Digital Ecosystems

Most of the MSMEs use third-party services, cloud storage, and SaaS tools to cut costs, but this raises compliance risks. They remain liable for vendor data breaches, which can lead to penalties. MSMEs face major compliance risks under the DPDPA due to third-party vendors handling data storage, SaaS tools, and payment processing.

While outsourcing reduces costs, MSMEs remain liable for vendor data breaches. Cloud storage on AWS, Google Cloud, or Azure can expose them to penalties if a breach occurs. SaaS tools for marketing, CRM, and analytics may process customer data without clear consent[9], leading to compliance violations. Payment gateways handle sensitive financial data, making them prime cyberattack targets.

Most of the MSMEs lack proper Data Processing Agreements (DPAs) and rely on informal terms, limiting legal recourse. Without audits, strict contracts, and security assessments, ensuring compliance remains a significant challenge.

4. Cross-Border Data Transfers & Business Operations[10]

MSMEs in e-commerce, IT outsourcing, digital marketing, and fintech face challenges under the DPDPA's cross-border data transfer restrictions, impacting operations and costs. Many rely on global cloud providers, payment processors, and foreign clients, but new regulations may disrupt operations. Data localization rules could force businesses to shift to Indian data centres, increasing costs. IT service providers risk losing international clients due to contractual and legal complications. Uncertainty over "trusted jurisdictions" further complicates planning, making compliance costly and complex for MSMEs without in-house legal expertise.

[9] Bhaswati Guha Majumder, "DPDP Draft Rules: Experts Highlight Challenges, Opportunities and Key Compliance Needs" (January 6 2025), available at: https://apacnewsnetwork.com/2025/01/dpdp-draft-rules-experts-highlight-challenges-opportunities-and-key-compliance-needs/#google_vignette (last accessed 16 March 2025).

[10] Krishnan Sreekumar, "DPDPA Compliance for Startups: Breaking Down the Essentials for Early-Stage Businesses in India" (17 August 2024), available at: https://ksandk.com/data-protection-and-data-privacy/dpdpa-startups/ (last accessed 16 March 2025).

STEP-BY-STEP DPDPA COMPLIANCE ROADMAP FOR STARTUPS & MSMEs

1. Identify and Map Personal Data across the Organization[11]

i. Identify Data Sources: Pinpoint where data is stored or originates, such as customer databases, employee records, vendor contracts, or third-party systems.
ii. Document Data Flow: Map how data moves within the organization and beyond, including who accesses it, for what purpose, and where it is transferred or stored.
iii. Categorize Data: Classify data into categories like sensitive personal data (e.g., financial or health information) and general data.

2. Conducting a Gap Analysis

i. Review Current Policies: Analyze existing privacy policies and procedures.
ii. Assess Data Handling Practices: Evaluate how data is collected, processed, and stored.
iii. Revise internal policies: After analyzing the gaps in the data collection practices, revised practices should be written in the privacy policies including the rights of the data principals.
iv. Review and Revise contractual clauses in 3rd party or Vendor contracts: Ensure that a data protection clause is incorporated in the commercial contracts between the startups, MSMEs, and the vendors or any 3rd party where data transfer is required in any capacity.
v. Highlight Gaps[12]: Identify areas that require improvement (e.g., consent mechanisms, technical controls).

3. Developing Data Protection Policies

i. Privacy Policy: Clearly communicate data collection and usage practices to individuals.
ii. Data Retention Policy: Define timelines and methods for retaining or deleting data.
iii. Incident Response Plans: Establish procedures for handling data breaches.
iv. Data Processing Agreement: Use DPAs when there is any transfer of data between any third party or any entity.

4. Implementing Technical Safeguards[13]

[11] Corridalegal,https://corridalegal.com/dpdp-act-compliance-guide-essential-steps-for-businesses/,(last visited March 13, 2025)
[12] Krishnan Sreekumar, DPDPA Compliance for Startups: Breaking Down the Essentials for Early-Stage Businesses in India, King Stubb & Kasiva,(last visited March 15, 2025),https://ksandk.com/data-protection-and-data-privacy/dpdpa-startups/
[13]T&R Law Offices,https://tandrlawoffices.in/navigating-data-breach-compliance-a-guide-for-startups-under-the-dpdp-act/ ,(last visited March 13, 2025)

i. Encryption: Safeguard sensitive data by converting it into an unreadable format during storage and transmission, ensuring only authorized parties with decryption keys can access it.
ii. Access Controls: Enhance role-based permissions and authentication mechanisms to restrict data access to authorized personnel, minimizing the risk of internal misuse or external threats.
iii. Pseudonymization: Enhance privacy by replacing personal identifiers with non-identifiable markers, making it harder to link data to individuals without additional information.
iv. Data Loss Prevention (DLP): Use tools and policies to monitor, detect, and prevent unauthorized data sharing or transfers, reducing the risk of accidental or malicious leaks.

5. Building a Governance Framework[14]

i. Appoint DPO: Designate a Data Protection Officer (DPO) to monitor compliance with privacy laws, advice on best practices, and act as appoint of contact for regulatory authorizes.
ii. Role of stakeholders: Clearly outline the duties and expectations for employees, managers, IT staff, and other stakeholders involved in data handling.
iii. Internal Audit: Regularly Implement regular internal audits to evaluate the effectiveness of data protection measures and compliance initiatives, identifying areas for improvement.
iv. Reporting Mechanism: Develop processes for documenting and reporting compliance efforts, incidents, and resolutions, enabling transparency and timely corrective actions.

6. Employees Training And Awareness Programs

i. Data handling best practices.
ii. Understanding the rights of the data principals.
iii. Recognizing and reporting data breaches.

Note: Effective training strategies include using real-life scenarios to make learning relatable and practical, enabling employees to apply concepts in real-world situations. Regular refresher courses ensure ongoing awareness of evolving compliance requirements and reinforce key principles. Together, these approaches create empowered employees who actively contribute to a culture of compliance and data protection.

[14] Vani Bhushan, International Journal of Advanced Research (IJAR),(last visited March 15, 2025),https://www.journalijar.com/article/48771/empowering-individuals:-a-deep-dive-into-the-digital-personal-data-protection-act,-2023/

7. Monitoring and Auditing for Compliance

i. Conduct regular internal[15] audits of data handling processes.
ii. Deploy automated tools to generate compliance reports.
iii. Analyze audit findings to identify and address gaps.

Note: Achieving continuous compliance improvement through regular evaluations and proactive measures ensures the organization remains aligned with evolving standards. This readiness fosters confidence and efficiency during regulatory inspections.

[15] *DPDPA Simplified from Scratch to Compliance*, Ministry of Security, https://www.youtube.com/watch?v=EtHgf_nXuoo

ISSUES MSMEs WILL FACE IN DPDPA COMPLIANCE & HOW THEY CAN NAVIGATE THESE CHALLENGES

Challenges MSMEs May Face in DPDPA Compliance[16]

1. Resource Constraints
   MSMEs often operate[17] with limited financial and human resources, making it difficult to allocate budgets for compliance programs, hiring a Data Protection Officer (DPO), and implementing advanced security measures.

2. Lack of Awareness and Expertise
   Many MSMEs may not fully[18] understand the complexities of DPDPA compliance, including the technical and legal aspects of data protection, leading to unintentional non-compliance.

3. Mapping and Managing Data Flows
   Identifying and tracking[19] personal data sources, transfers, and storage locations across different systems can be challenging, especially for businesses using outdated or fragmented data management systems.

4. Ensuring Robust Consent Mechanism
   Obtaining and managing[20] consent from data principals (customers, employees, vendors) in a structured and legally compliant manner can be complex, particularly for businesses with high volumes of transactions.

5. Implementing Technical Safeguards
   Deploying encryption, access controls, pseudonymization, and data loss prevention (DLP) tools may require significant investment in cybersecurity infrastructure, which MSMEs may struggle to afford.

6. Developing Data Protection Policies and Governance Framework
   MSMEs may lack standardized policies[21] for data retention, breach response, and overall governance, making them more vulnerable to regulatory violations.

---

[16] Adv. Yatin Pandit, International Journal of Advanced Research (IJAR),(last visited March 14, 2025),https://www.ijrar.org/papers/IJRAR1DOP002.pdf
[17] 5 Data Privacy Strategies Every MSME Needs in 2025, https://protium.co.in/5-data-privacy-strategies-every-msme-needs-in-2025/
[18] Ibid
[19] Top 10 operational impacts of India's DPDPA – Enforcement and the Data Protection Board, https://iapp.org/resources/article/operational-impacts-of-indias-dpdpa-part4/?utm_source=chatgpt.com
[20] Ibid
[21] India's Data Protection Bill: Impacts on India's MSME Sector, https://www.bimakavach.com/blog/indias-data-protection-bill-impacts-on-indias-msme-sector/?utm_source=chatgpt.com

7. Employee Awareness and Training
   Employees handling personal data may not be adequately trained in data protection best practices, leading to accidental data breaches or non-compliance with DPDPA requirements.

8. Regular Monitoring and Auditing
   Conducting frequent compliance audits[22] and generating reports requires dedicated personnel and automated tools, which many MSMEs may not have access to.

How MSMEs Can Navigate DPDPA Compliance Challenges[23]

1. Prioritizing a Phased Approach
   MSMEs can adopt a step-by-step compliance strategy, starting[24] with high-risk areas such as data storage, consent mechanisms, and encryption, and gradually expanding compliance efforts as resources allow.

2. Utilizing Cost-Effective Tech Solutions
   Cloud-based compliance tools[25], free cybersecurity frameworks, and affordable solutions can help MSMEs enhance data protection without excessive financial burdens.

3. Outsourcing Data Protection Responsibilities (DPOs, External Consultants)
   Instead of hiring[26] an in-house DPO, MSMEs can engage external consultants or legal advisors to ensure compliance while optimizing costs.

4. Implementing Simplified Data Management Practices
   Businesses should focus[27] on data minimization—collecting only necessary information—and using automated tools for data mapping and documentation.

5. Developing a Scalable Compliance Framework

[22] Ibid
[23] T&R Law Offices,https://tandrlawoffices.in/navigating-data-breach-compliance-a-guide-for-startups-under-the-dpdp-act/ ,(last visited March 13, 2025)
[24] The Digital Personal Data Protection Act, 2023: Opportunities and Compliance Strategies for Businesses, https://dpdpa.com/blogs/opportunities_small_business_dpdpa.html?utm_source=chatgpt.com
[25] Ibid
[26] Strategic Support for DPDPA Compliance, Verasafe, https://verasafe.com/advisory-and-audit/india-dpdp-act-compliance/?utm_source=chatgpt.com
[27] The Digital Personal Data Protection Act, 2023: Opportunities and Compliance Strategies for Businesses, https://dpdpa.com/blogs/opportunities_small_business_dpdpa.html?utm_source=chatgpt.com

MSMEs should create simple, adaptable privacy policies, establish a basic incident response plan, and maintain clear records of compliance efforts to demonstrate good faith in case of regulatory scrutiny.

6. Investing in Employee Awareness and Training
   Conducting short, practical training sessions with real-life case studies can help employees understand their role in data protection and compliance.

7. Adopting a Proactive Monitoring and Auditing Approach
   Regular internal reviews, using automated reporting tools where possible, will help MSMEs identify risks early and address them before they escalate into compliance violations.

By addressing these challenges strategically, MSMEs can effectively align with DPDPA compliance requirements while balancing their operational constraints.

COST-EFFECTIVE COMPLIANCE STRATEGIES FOR STARTUPS & MSMES

1. Low-Cost and Open-Source Compliance Tools for Privacy Management

Startups and MSMEs in India may face a significant budgetary and resource constraints when implementing compliance measures under the Digital Personal Data Protection Act (DPDPA), 2023. In this context, open-source solutions emerge as attractive options for privacy management, offering the dual benefits of cost efficiency and high customizability. Open-source tools can be adopted without incurring expensive licensing fees while also allowing organizations to tailor functionalities to their specific compliance needs[28].

A. Rationale for Open-Source Approaches

Small- and medium-sized enterprises typically lack the in-house legal and technical expertise that large corporations enjoy[29]. As a result, they can rely on cost-effective and easily deployable solutions to manage privacy compliance. Open-source tools, developed and continuously improved by global communities, provide a viable solution. They not only reduce the initial investment costs but also offer the flexibility to integrate with existing IT infrastructures and customize functionalities according to specific regulatory requirements[30].

B. Evaluated Open-Source Tools and Their Features

Recent academic evaluations have shed light on a number of open-source tools that are particularly promising for privacy management:

i. Differential Privacy Tools: Differential privacy frameworks add a calibrated amount of noise to data to preserve individual privacy. There are several open-source differential privacy tools such as OpenDP Smartnoise[31], PyTorch Opacus[32], TensorFlow

[28] lexpanacea.in, Cost-Effective Compliance Solutions: Navigating the DPDPA for Startups - Lexpanacea.in Cost-Effective Compliance Solutions: Navigating the DPDPA for Start-Ups, (May 24, 2024), https://lexpanacea.in/cost-effective-compliance-solutions-navigating-the-dpdpa-for-startups/ (last visited Mar 17, 2025); Martin Brodin, A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises, 4 Eur J Secur Res 243, 244 (2019).
[29] Brodin, supra note 1 at 244.
[30] Maria Da Conceição Freitas & Miguel Mira Da Silva, GDPR Compliance in SMEs: There Is Much to Be Done, 3 Journal of Information Systems Engineering & Management, 2 (2018), http://www.jisem-journal.com/article/gdpr-compliance-in-smes-there-is-much-to-be-done-3941 (last visited Mar 17, 2025).
[31] https://docs.smartnoise.org/
[32] https://opacus.ai/

Privacy[33], and [34]Diffprivlib.[35] These tools balance the trade-off between privacy protection and data utility by quantifying privacy loss with parameters like ε (epsilon). Their empirical evaluation indicates that such tools can be effectively deployed in settings with limited resources, making them suitable for SMEs that require cost-efficient yet robust privacy protection mechanisms.

ii. Encryption and Data Masking Solutions: Open-source encryption tools such as VeraCrypt[36] and GnuPG[37] provide robust data protection for data at rest and in transit at minimal cost. Additionally, tools for data masking have been successfully used to protect sensitive information during testing and development, ensuring that even if data is accessed unlawfully, it remains unintelligible[38].

iii. Network Security and Firewall Tools: Free solutions like pfSense[39] offer comprehensive firewall capabilities. Such tools are essential for preventing unauthorized access to sensitive data and can be deployed on commodity hardware, thus reducing the overall cost of compliance infrastructure.

iv. Consent Management and Data Mapping Tools: Although traditionally proprietary solutions exist for managing user consent and data mapping, open-source alternatives have been emerging. These tools enable organizations to maintain transparency regarding data flows and consent practices without the need for heavy financial investment[40].

C. Integration and Customization within Existing Infrastructures

One of the significant advantages of open-source solutions is their adaptability to diverse operating environments. Startups and MSMEs can integrate these tools into their existing IT infrastructure, often with minimal disruption. For instance, the modular design of many open-source platforms allows organizations to adopt only the necessary components—such as encryption modules, firewall protection, or differential privacy mechanisms—thus optimizing resource allocation[41]. Moreover, the inherent transparency of open-source software facilitates auditing and customization, enabling organizations to adjust the tools to better align with the specific compliance mandates of the DPDPA[42].

[33] https://www.tensorflow.org/
[34] https://diffprivlib.readthedocs.io/en/latest/
[35] Shiliang Zhang et al., Evaluation of Open-Source Tools for Differential Privacy, 23 SENSORS 6509, 2–3 (2023).
[36] https://www.veracrypt.fr/en/Home.html
[37] https://gnupg.org/
[38] Brodin, supra note 1.
[39] https://www.pfsense.org/
[40] Freitas and Mira Da Silva, supra note 3 at 2.
[41] Brodin, supra note 1.
[42] lexpanacea.in, supra note 1.

2. Affordable Outsourcing of DPDPA Compliance

Outsourcing data protection compliance can be an effective way for startups to fulfil legal obligations while minimizing costs. The following strategies can help:

A. Partnering with Compliance-as-a-Service (CaaS) Providers
Many firms offer end-to-end compliance solutions tailored for MSMEs and startups. These providers manage policy implementation, data security audits, and regulatory reporting at a fraction of the cost of an in-house team.[43] Leveraging such services can help startups meet DPDPA requirements efficiently without investing in full-time personnel.[44]

B. Cloud-Based Compliance Solutions
Startups can use cloud compliance management tools that offer automated data mapping, risk assessment, and documentation.[45] These tools help maintain compliance by regularly updating policies based on regulatory changes.

C. Engaging External Data Protection Officers (DPOs) on a Contract Basis
Instead of hiring a full-time DPO, startups can engage an external consultant on a retainer basis. This allows compliance guidance without a long-term salary commitment. External DPOs assist with privacy impact assessments, policy documentation, and incident response planning.[46]

D. Legal and Compliance Outsourcing Firms
Engaging legal firms with expertise in DPDPA compliance helps in interpreting legal mandates and drafting necessary documentation. These firms can assist with drafting Data Processing Agreements (DPAs) and Privacy Notices, which are crucial for regulatory adherence.

3. Building an Internal Data Protection Framework Without a Full Compliance Team

A. Organisational Commitment and Leadership Involvement

[43] Effective Cost Management Strategies for Startups rryge June 28, 2024
https://ssnifound.in/2024/06/28/effective-cost-management-strategies-for-startups/
[44]GIZ Compliance Tool kit For Startups
https://www.allianceforintegrity.org/wAssets/docs/publications/en/compliance-programme/GIZ_ComplianceToolkitForStartups_Final-v1.8-WEB.pdf
[45] Compliance plays a big part in helping Indian MSMEs grow exports, Ashish Pandey,
https://economictimes.indiatimes.com/small-biz/sme-sector/compliance-plays-a-big-part-in-helping-indian-msmes-grow-its-exports/articleshow/110164887.cms?from=mdr
[46] ibid

Leadership commitment is the foundation of an effective compliance programme. Founders and senior management must take ownership of data protection policies, ensuring that compliance is embedded within business operations.[47] Establishing a clear data protection policy that outlines key principles, responsibilities, and accountability measures is essential. Leadership should designate a data protection lead (DPL) from existing team members, rather than hiring a full compliance team.

B. Defining the Data Protection Framework

Once risks are identified, an internal data protection framework should be developed and documented. This includes[48]

I. Data Classification & Inventory – Mapping data flows within the organization, categorizing data based on sensitivity, and defining access controls.

II. Data Collection and Processing Policies – Clearly defining the purpose and lawful basis for data collection, ensuring minimal and necessary data processing.

III. Security and Access Controls – Implementing role-based access and encryption mechanisms to safeguard personal data.

IV. Consent Management – Ensuring valid and explicit consent is obtained before collecting personal data.

V. Data Retention and Deletion – Establishing guidelines for data storage duration and secure deletion mechanisms.

C. Leveraging ICT and Automation for Compliance

To reduce manual compliance efforts, startups should invest in cost-effective compliance automation tools, such as:[49] Enterprise Resource Planning (ERP) systems to streamline compliance processes, Privacy Management Software for automated data classification and monitoring, Open-source risk assessment tools to evaluate security vulnerabilities. By using low-cost digital solutions, startups can significantly reduce the burden of manual compliance tracking.

D. Internal Audits and Monitoring

[47] GIZ Compliance Tool kit For Startups https://www.allianceforintegrity.org/wAssets/docs/publications/en/compliance-programme/GIZ_ComplianceToolkitForStartups_Final-v1.8-WEB.pdf

[48] Id at 5.
[49] Ibid

Continuous monitoring and evaluation are critical to maintaining data protection compliance. Startups should:

i. Conduct periodic internal audits to assess data protection measures.
ii. Establish a reporting mechanism for employees to flag data protection issues confidentially.
iii. Set up a whistleblower protection policy to encourage reporting of non-compliance incidents without fear of retaliation.

WHY DATA PROTECTION MATTERS FOR STARTUPS AND MSMEs?

In today's rapidly evolving[50] digital landscape, data is the backbone of innovation, decision-making, and business operations for startups and MSMEs. However, the growing reliance on sensitive personal and financial information, coupled with rising concerns around privacy, underscores the need for strong data protection practices. Protecting user data isn't just a matter of legal compliance—it's essential for building customer trust, avoiding significant financial losses, and ensuring long-term business continuity. As businesses collect, process, and store vast amounts of personal data, the risks of fraud, identity theft, and cyber-attacks are ever-present, making data protection more critical than ever. Here's why startups and MSMEs must prioritize data protection:[51]

1. Building Customer Trust and Loyalty: A strong data protection strategy helps establish credibility and fosters trust with customers, which can lead to sustained business relationships and growth.

2. Avoiding Financial Loss, Penalties, and Fines: Data breaches can lead to significant financial consequences, including fines and legal liabilities. For example, Meta faced a €1.2 billion[52] fine for breaching data protection laws. Startups and MSMEs must ensure compliance to avoid these costly repercussions.

3. Preventing Fraud and Identity Theft: If user data falls into the wrong hands, it can lead to fraud or identity theft. This not only damages individuals but also creates a major legal and reputational challenge for businesses in defending the breach.

4. Ensuring Legal Compliance: Compliance with laws such as the Digital Personal Data Protection Act (DPDPA) and GDPR is mandatory. Failure to adhere to these regulations

[50] 15 things all small businesses need to know about data protection (2023) ico.org.uk. Available at: https://ico.org.uk/for-organisations/advice-for-small-organisations/whats-new/blogs/15-things-all-small-businesses-need-to-know-about-data-protection/
[51] Martin, N., Matt, C., Niebel, C. et al. How Data Protection Regulation Affects Startup Innovation. Inf Syst Front 21, 1307–1324 (2019). https://doi.org/10.1007/s10796-019-09974-2
[52] https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en#:~:text=Brussels%2C%2022%20May%20%2D%20Following%20the,Protection%20Authority%20(IE%20DPA).

can result in hefty fines, legal actions, and reputational damage, posing a serious threat to business operations.

5. Protecting Reputation and Brand Integrity: Repeated data breaches can harm a startup's reputation, diminishing consumer confidence. A failure to protect sensitive data might cause customers to hesitate in doing business with a company, leading to a loss of market share and trust.

6. Securing Business Continuity: Data is essential to business operations, and protecting it ensures continuity even during disruptions such as cyber-attacks or natural disasters. Effective data protection allows businesses to recover quickly and continue serving their customers.

7. Gaining Competitive Advantage: Data security can be a key differentiator in industries where privacy is paramount. Startups that prioritize data protection can attract customers who value privacy, creating a competitive edge in a crowded marketplace.

8. Facilitating Global Expansion: As MSMEs expand into international markets, complying with stringent data protection standards becomes necessary. Many global markets and partners require businesses to meet specific data privacy regulations, enabling MSMEs to access new growth opportunities.

9. Protecting Against Cyber-Attacks: Cyber-attacks pose a real threat to MSMEs, which are often viewed as more vulnerable targets. Implementing strong data protection practices helps safeguard against attacks, reducing the risk of data theft and operational disruptions.

10. Meeting Investor Expectations: Investors are increasingly focused on a company's ability to protect sensitive data. Demonstrating a commitment to data protection and compliance with privacy regulations signals to investors that the business is well-managed and capable of mitigating potential risks.

11. Minimizing Legal and Reputational Risks: Non-compliance with data protection laws can expose startups to legal challenges and lawsuits, leading to financial and reputational damage. Safeguarding data and complying with data protection laws can help avoid these risks and ensure smoother business operations.

The Increasing Regulatory Focus on Data Privacy in India

In recent years, data privacy[53] has become a focal point for regulators around the world, and India is no exception. The country has witnessed an increasing push towards stricter data

[53] Digital Personal Data Protection Act: Shaping India's AI-driven fintech sector (2025) orfonline.org. Available at: https://www.orfonline.org/english/expert-speak/digital-personal-data-protection-act-shaping-india-s-ai-driven-fintech-sector

privacy laws, culminating in the introduction of the Digital Personal Data Protection Act (DPDPA) 2023. This shift reflects the global trend towards recognizing the importance of protecting individuals' personal data and ensuring transparency in how it is handled. With the exponential rise of data collection, analytics, and digital transactions, regulators in India have recognized that data privacy is no longer just a matter of business ethics but a legal imperative. The Indian government's push to adopt comprehensive data protection laws underscores the growing concerns over privacy violations and the need to establish a robust framework that can help businesses stay compliant while safeguarding user data.

Why Data Privacy Compliance Is Critical for Startups & MSMEs—Beyond Legal Risk?

For startups and MSMEs, complying[54] with data privacy laws is not just about avoiding legal trouble; it has far-reaching implications for customer trust, business growth, and even funding opportunities. Here's why data privacy compliance is so important:

1. Customer Trust and Brand Reputation

Trust is the cornerstone of any business, particularly for startups that are still building their brand. In a digital-first world, customers are increasingly aware of how their personal data is handled. Companies that prioritize data privacy are viewed as more trustworthy, and this can significantly impact customer loyalty. On the flip side, data breaches or mishandling of personal data can lead to loss of customer confidence, tarnishing the brand and driving users to competitors.

2. Business Growth and Competitive Advantage

Adhering to data privacy laws can be a strategic differentiator. In an increasingly crowded market, customers are more likely to choose businesses that demonstrate a commitment to protecting their personal information. Furthermore, data privacy compliance enables startups to expand into new markets, as many regions, such as the European Union and the United States, require businesses to comply with specific data protection laws before they can operate or offer services.

3. Investor Confidence and Funding

Investors are more likely to back startups that have a strong data protection framework in place. The increasing scrutiny of data privacy by investors, particularly in sectors dealing with sensitive personal information, means that a robust compliance program could directly influence funding decisions. Companies with poor data management

[54] IBM (2015) Why data privacy is much more than compliance, IBM. Available at: https://www.ibm.com/security/digital-assets/data-privacy-matters/

practices or that are subject to regulatory penalties could present higher risks for investors.

4. Long-Term Business Sustainability

Complying with data privacy regulations ensures business continuity in the long run. Data breaches and non-compliance with data protection laws can lead to heavy fines, legal battles, and long-lasting reputational damage that may make it difficult for startups to recover. By establishing compliance protocols early on, startups and MSMEs safeguard themselves against such risks, enabling them to focus on growth and scaling operations.

COMPARISON OF GLOBAL PRIVACY LAWS (GDPR, CCPA) VS. INDIA'S DPDPA

The Digital Personal Data Protection Act, 2023 (DPDPA) marks a significant step in India's data protection landscape[55], aligning itself with global privacy frameworks like the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) while also incorporating India-specific nuances. This comparison highlights the similarities and key differences across these regulatory frameworks and evaluates where India stands in the global data protection ecosystem.

GDPR	CCPA	DPDPA
Scope & Coverage		
• Applies to all personal data, whether digital or physical, as long as it is part of a structured filing system. • Encompasses data processing by entities within the European Economic Area (EEA) and any organization globally that offers goods or services to EU citizens	• Focuses on consumer rights, applying to for-profit businesses that meet certain thresholds (e.g., annual revenue over $25M, processing data of more than 50,000 California residents). • Covers household and device data, in addition to personal information of individuals.	• Applies only to digital personal data and excludes publicly available data from its scope. • Covers businesses operating in India and those outside India if they process data related to offering goods/services in India.
Categorization of Personal Data		
Recognizes special categories of sensitive data, including racial/ethnic origin, religious beliefs, health, biometric data, political views, and sexual orientation	Introduces sensitive personal information, such as financial data, social security numbers, geolocation, and genetic information.	Does not specifically classify sensitive data but allows the government to impose additional obligations on certain types of data processing.
Legal Basis for Processing		
Provides six legal bases for processing, including	Primarily follows an opt-out model, allowing businesses	Heavily consent-driven, with limited legitimate uses

[55] Soni, A.P., Arpita Sengupta, Anoushka (2024) Comparing Global Privacy Regimes Under GDPR, DPDPA and US Data Protection Laws, India Corporate Law. Available at: https://corporate.cyrilamarchandblogs.com/2024/01/comparing-global-privacy-regimes-under-gdpr-dpdpa-and-us-data-protection-laws/

legitimate interests, contractual necessity, compliance with legal obligations, and consent	to process data unless users explicitly request to opt out.	(such as compliance with laws, employment-related processing, or voluntary provision by the user). Does not include the broad legitimate interest ground that GDPR provides
Processing of Children's Data		
Sets the age of consent between 13–16 years, depending on the member state. Requires reasonable efforts to obtain parental consent.	Allows opt-in consent for data sales for minors aged 13-16; requires parental consent for children under 13.	Sets the age of consent at 18, requiring verifiable parental consent for all processing. Explicitly bans behavioral tracking, targeted advertising, and any processing that may harm the child
Data Breach Notification		
Requires notification to the regulator within 72 hours if the breach poses a risk to individual rights. Only high-risk breaches need to be reported to individuals.	Requires notification to affected individuals but no strict timeframe for reporting	Mandates reporting all breaches to both the Data Protection Board (DPB) and affected users. Specific reporting timelines will be prescribed in the rules.
Cross-Border Data Transfers		
Uses a whitelist approach—data can be transferred to countries that ensure adequate protection or through legal safeguards (SCCs, BCRs).	No strict cross-border restrictions but mandates transparency on data sharing	Uses a blacklist approach—data transfers are allowed unless the government explicitly prohibits certain countries.
Grievance Redressal & Enforcement		
Individuals can file complaints directly with regulatory authorities or approach courts	Allows consumers to sue businesses in case of a data breach but does not grant a private right of action for general violations	Users must first seek redress from the Data Fiduciary before escalating complaints to the Data Protection Board (DPB)

Rights of Data Subjects			
Rights	GDPR	CCPA	DPDPA
Access to data	✅ Yes	✅ Yes	✅ Yes
Right to rectification	✅ Yes	❌ No	✅ Yes
Right to erasure	✅ Yes ("Right to be Forgotten")	✅ Yes (for some cases)	✅ Yes
Data portability	✅ Yes	✅ Yes	❌ No
Opt-out of processing	✅ Yes	✅ Yes	❌ No (Except in withdrawal of consent)

Where India Stands in the Global Data Protection Landscape

The Digital Personal Data Protection Act, 2023 (DPDPA) represents a significant milestone in India's data protection framework, aligning with global privacy standards while incorporating unique domestic considerations. Compared to the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA),[56] the DPDPA is more consent-centric, offering individuals greater control over their personal data. However, unlike GDPR, which provides multiple legal bases for data processing, the DPDPA primarily relies on explicit consent with limited exceptions under legitimate uses. This makes the Indian framework stricter in requiring user approval but potentially more cumbersome for businesses that rely on flexible processing mechanisms like legitimate interests under GDPR.

One of the key areas where India diverges from other global laws is in the protection of children's data. The DPDPA sets 18 years as the age of consent, significantly higher than the 13-16 year range under GDPR and CCPA, and introduces strict bans on tracking, targeted

[56] LLP, L. & W. (2023) India's Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison, Global Privacy & Security Compliance Law Blog. Available at: https://www.globalprivacyblog.com/2023/12/indias-digital-personal-data-protection-act-2023-vs-the-gdpr-a-comparison/

advertising, and behavioral monitoring of minors. While this enhances child safety, it also imposes operational challenges for businesses that cater to younger users, necessitating stringent age verification and parental consent mechanisms.

In terms of cross-border data transfers, India has opted for a blacklist approach, allowing free data transfers except to countries that may be explicitly restricted by the government. This contrasts with GDPR's whitelist model, which only allows transfers to jurisdictions that meet strict adequacy standards. While this provides greater flexibility for businesses operating in India, future government-imposed restrictions could affect data flows and compliance strategies. Another significant distinction is the data retention framework under the DPDPA. Unlike GDPR, where organizations determine retention periods based on necessity, the DPDPA is expected to define specific timelines through upcoming rules, reducing flexibility for businesses.

The DPDPA also introduces a unique concept of Consent Managers, a regulatory mechanism absent in GDPR and CCPA. These registered intermediaries will facilitate the granting, review, and withdrawal of consent, thereby empowering data principals with enhanced transparency and control over their personal information. However, in contrast to GDPR's direct obligations on data processors, the DPDPA does not impose direct accountability on processors, placing the entire compliance burden on data fiduciaries (controllers). This increases contractual risks for businesses engaging third-party service providers and necessitates stronger data processing agreements.

Another notable difference is in data breach reporting. The DPDPA mandates reporting of all breaches to both the Data Protection Board (DPB) and affected users, whereas GDPR requires reporting only if a breach poses a high risk to individuals. This increases compliance responsibilities for organizations in India, making incident response planning crucial. Additionally, grievance redressal under the DPDPA follows a tiered approach, requiring data principals to first seek resolution from the data fiduciary before escalating complaints to the DPB, unlike GDPR, which allows direct complaints to the supervisory authority.

Overall, while the DPDPA shares core principles with GDPR and CCPA—such as transparency, purpose limitation, and data minimization—it deviates in its execution, balancing privacy rights with regulatory oversight. It reflects India's unique approach to data governance, ensuring individual data protection while considering the needs of businesses and the government. Companies operating in India must carefully assess the nuances of the DPDPA, update their compliance programs, and adapt data governance strategies accordingly. With future rules yet to be framed, ongoing engagement with regulatory developments will be essential for businesses to successfully navigate India's evolving data protection landscape.[57]

[57] India's Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison (2023). Available at: https://www.lw.com/admin/upload/SiteAttachments/Indias-Digital-Personal-Data-Protection-Act-2023-vs-the-GDPR-A-Comparison.pdf.

ENFORCEMENT & CASE STUDIES: LEARNING FROM INDUSTRY MISTAKES

The IT Act, 2000 was the primary law dealing with cybercrimes but the introduction of DPDP Act, 2023 has completely overhauled India's outlook towards data breaches and the remedies thereof. The recent data breaches have significantly pressed the need of urgent implementation of the Act.

In recent years, India has increasingly focused its regulatory environment on startups, especially due to growing concerns around data privacy and protection. As India prepares for the full implementation of the Digital Personal Data Protection Act (DPDPA), the mistakes made by startups in the past offer valuable lessons on how to handle compliance moving forward.

THE VULNERABLE STATE OF INDIAN COMPANIES

BSNL Data Breach

In May 2024, BSNL suffered a huge data resulting in loss of 278 GB of sensitive data, which included details such as IMSI numbers, SIM card details and home location register. The breach came into light when a US person put the data to sell on dark web.[58] Another incident of data breach of such great extent of Boat wherein personal information 7.2 million boat users were sold on dark web, the personal information included the name, mobile numbers, address and email addresses of the customers[59].

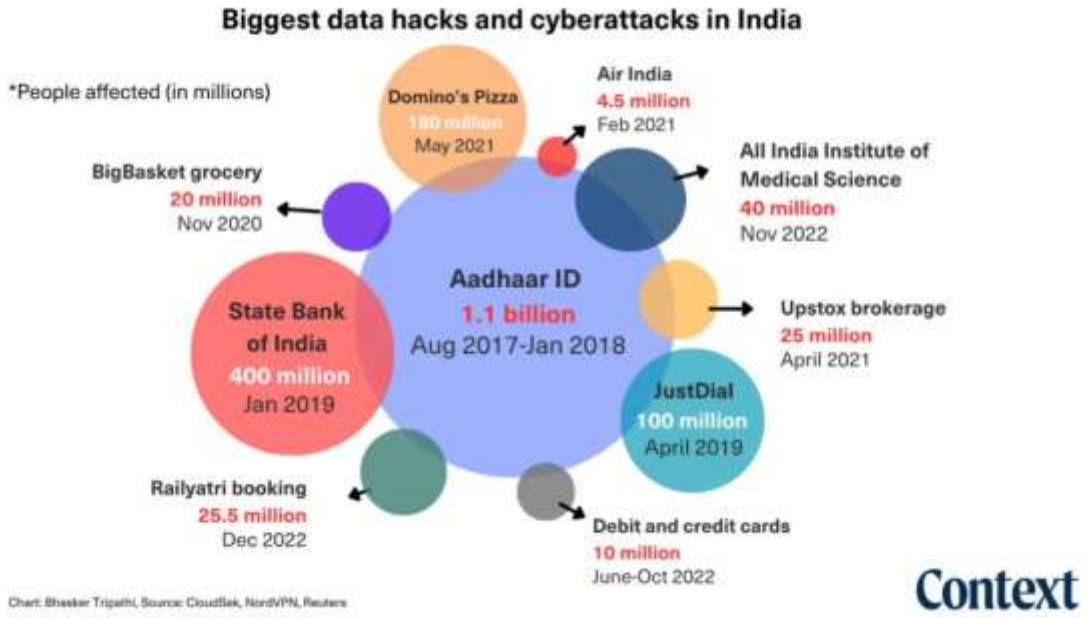
OLA Data Breach

Furthermore, back in 2014, Ola Cabs experienced a significant security incident when a hacker group named 'TeamUnknown' claimed to have accessed sensitive user data, including credit card transaction histories and unused vouchers. The attackers exploited vulnerabilities in Ola's development server, which was inadequately secured[60]. This incident underscored the necessity for robust security measures, even in non-production environments, to maintain user trust and comply with data protection standards.

Zomato Data Breach

[58] https://www.hindustantimes.com/india-news/us-hacker-likely-linked-to-24-bsnl-data-breach-101736449217788.html
[5959] https://www.business-standard.com/companies/news/boat-suffers-data-breach-personal-data-of-75-lakh-users-leaked-on-dark-web-124040801022_1.html
[60] https://www.bankinfosecurity.asia/blogs/ola-cabs-hack-analysis-p-1874

In 2017, Zomato experienced a significant data breach affecting over 17 million users, exposing email addresses and hashed passwords. The breach was attributed to human error, where an employee's development account was compromised, leading to unauthorized access to the database[61].



These recent data breaches have not only compromised the security of users' personal information but have also had a detrimental impact on the company's brand reputation, creating substantial challenges in regaining investor confidence and attracting potential investments. These cases shows that the companies had weak security safeguards and are not up to date with the recent safety requirements of the DPDP Act, though it is still not in force but companies should be ready to make their policies as per the requirements of the Act.

In contrast to other companies that failed to acknowledge their data breaches, Zomato demonstrated transparency by promptly informing users about the incident. The company communicated that the compromised data included email addresses and hashed passwords[62] and assured users that payment information was securely stored separately and remained

[61] http://economictimes.indiatimes.com/small-biz/security-tech/security/zomato-hacked-security-breach-results-in-17-million-user-data-stolen/articleshow/58729251.cms?from=mdr
[62] https://blog.zomato.com/security-update-what-really-happened-and-what

unaffected. Zomato also reset passwords for all affected users and enhanced security measures to prevent future breaches[63].

LEARNINGS FROM THE GLOBAL CASES OF DATA BREACH

Meta Data Breach (2018)

In December 2024, the Irish Data Protection Commission fined Meta €251 million for a 2018 data breach that exposed personal information of approximately 29 million Facebook users globally. The breach resulted from unauthorized access to user tokens, compromising data such as names, contact details, and other sensitive information[64]. The DPC found that Meta's practices violated several GDPR provisions, including Articles 33(3), 33(5), 25(1), and 25(2), leading to substantial fine. These provisions put obligations on Meta to document breach details, to collect only necessary data, providing breach information etc.

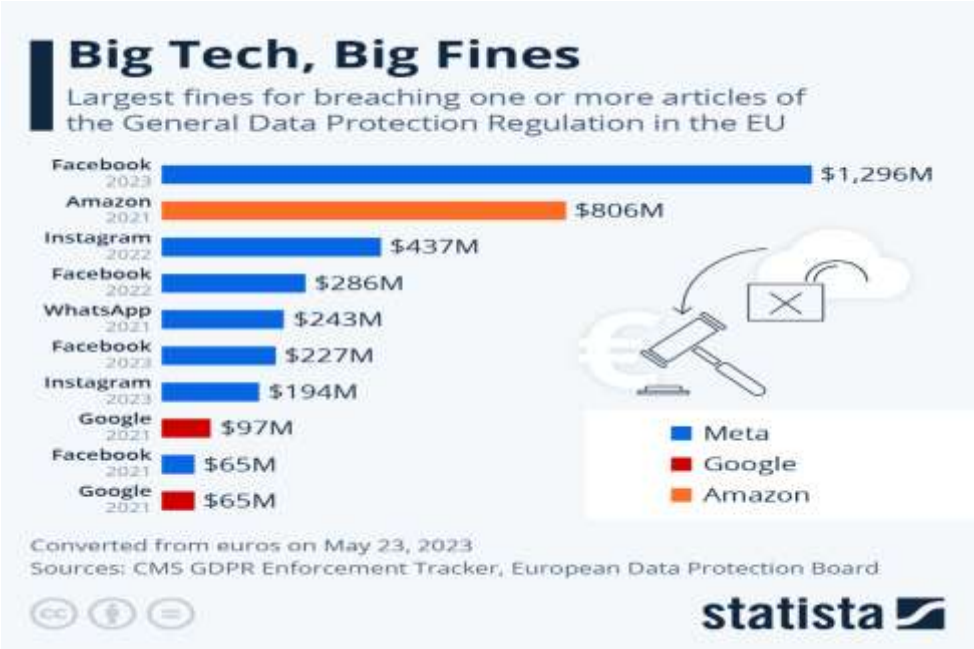
WhatsApp Data Breach

The €225m fine is the second largest fine, which is imposed under EU GDPR[65]. WhatsApp violated the provisions of free consent and transparency of processing personal data (Art.6)[66]

Tiktok Data Breach

Tiktok was fined €345m by the Irish DPC over handling the children's data. During 2020, Tiktok by default made the account public, which the children aged between 13-17 years created[67]. The company was ordered to adjust its data processing practices to comply with GDPR within three months.[68]

[63] https://economictimes.indiatimes.com/small-biz/security-tech/security/zomato-hacked-security-breach-results-in-17-million-user-data-stolen/articleshow/58729251.cms?from=mdr
[64] https://www.dataprotection.ie/en/news-media/press-releases/irish-data-protection-commission-fines-meta-eu251-million
[65] https://www.bbc.com/news/technology-58422465
[66] https://www.dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-inquiry-whatsapp
[67] https://www.bbc.com/news/technology-66819174
[68] https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-345-million-euro-fine-of-TikTok



By analysing, the above cases one thing is clear that there were clear violation of the GDPR regulations and the companies did not had a robust security safeguards and contemplated by the GDPR. Going by the provisions, huge fines were imposed on all these giants. Indian companies have a lot to learn from the mistakes of these companies to ensure that they do not get their data breached.

One thing is for sure that the Indian startups need an urgent revamp of their data privacy safeguards to bring them in line with the DPDP Act, 2023 and the rules. It should mainly focus on consent notice, notification of data breach and processing of children's data.[69]

It is clear that there will be significant fines for any breach committed under DPDP Act, just as the case with GDPR. It is advisable that the companies should ensure alignment with the Act.

Key Learnings for Indian Startups

1. Prioritize user consent and ensure clarity in privacy policies.
2. Regularly conduct security audits and penetration testing to safeguard data.
3. Implement robust data protection measures, particularly for sensitive personal and payment data.
4. Immediate breach notification and transparent communication with users are crucial.
5. Compliance with global standards such as GDPR will be critical for startups with international operations.

[69] https://www.azbpartners.com/bank/digital-personal-data-protection-act-2023-key-highlights/

CONCLUSION

The Digital Personal Data Protection Act, 2023 (DPDPA) aligns with global data protection frameworks and establishes a strong foundation for India's data protection regime. The Act mandates compliance across all sectors, placing the responsibility of handling digital data on businesses.

For startups and MSMEs, data protection is critical to ensuring customer trust, regulatory compliance, financial security, and business continuity. With rising cyber threats and stringent global regulations like GDPR, CCPA, and India's DPDPA, businesses must implement robust security measures to mitigate risks, avoid penalties, and safeguard their reputation.

While DPDPA 2023 aligns with global standards, it is highly consent-driven, imposes stricter regulations on children's data, and introduces unique enforcement mechanisms. Recent data breaches (e.g., BSNL, Boat, Zomato) underscore the urgent need for stronger security practices. Learning from global cases involving Meta, WhatsApp, and TikTok, businesses must proactively adopt data protection frameworks to ensure compliance and long-term sustainability.

For MSMEs, integrating data protection from the outset is crucial to avoiding legal complications, hefty fines, and reputational damage. Implementing encryption, access controls, and transparent consent mechanisms can strengthen security. However, resource constraints, lack of awareness, vendor risks, and cross-border data regulations pose significant challenges for small businesses.

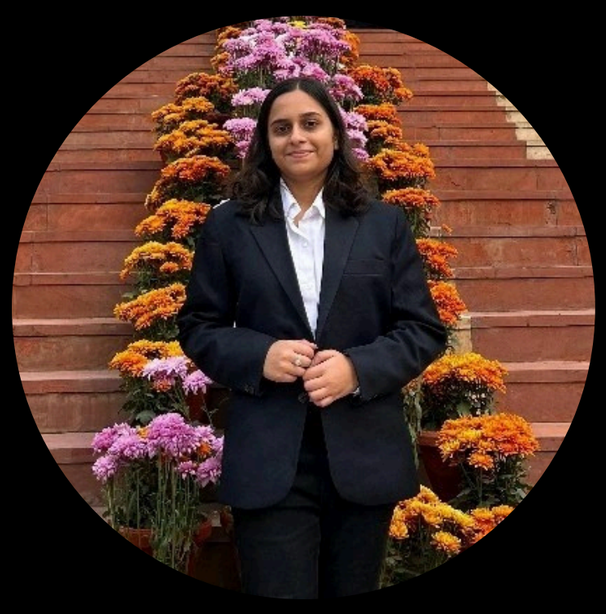
Potential exemptions for MSMEs could provide some relief, but clear regulatory guidelines and accessible compliance resources are essential. Developing tailored data protection policies that address the specific needs of MSMEs will help them thrive in India's digital economy. As data privacy becomes a competitive advantage, MSMEs that proactively integrate compliance measures will be better positioned for sustainable growth in an increasingly regulated digital landscape.

KEY CONTRIBUTORS

Dr. Md Safiullah
Faculty Convenor
CIILE

Manvee
Student Convenor
CIILE & Founder-LL.B Mania

Adil Ameen
Editor-in-Chief
CIILE



Aarya Gurjar
Deputy Secretary
CIILE

Khushi Gupta
Associate Editor
CIILE

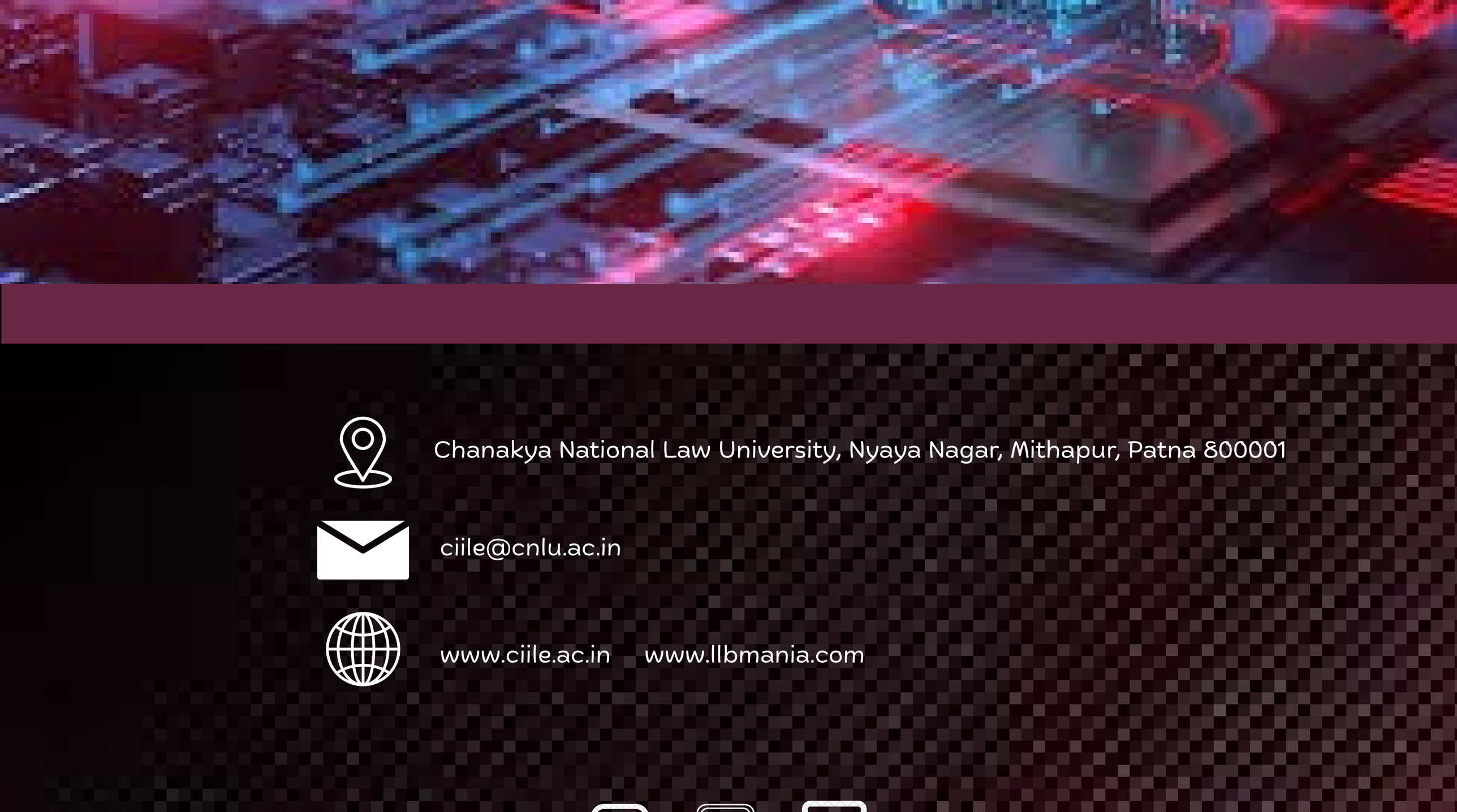
Aditya Kumar
Associate Editor
CIILE

Sakshi Kumari
Associate Editor
CIILE

Garima Bairagi
Associate Editor
LL.B Mania

Samridhi
Copy Editor
CIILE

Saumya Sudarshini
Copy Editor - CIILE
& Member-LL.B Mania



Chanakya National Law University, Nyaya Nagar, Mithapur, Patna 800001

ciile@cnlu.ac.in

www.ciile.ac.in www.llbmania.com