A Quarterly insight to Cyber Law!

Cyber Niyam means rules of the Cyberspace. This quarterly newsletter aims to create awareness about the rules and regulations of cyberspace, cyber security and data protection. This is also an effort to create awareness about digital safety, trending cybercrimes and effective reporting mechanisms.

Disclaimer

CYBER NIYAM

By Adv. Vaishali Bhagwat *www.vaishalibhagwat.com*

Issue 1 of 2026 – January, 2026

In this Issue

WHY SHOULD ORGANIZATIONS CARE ABOUT DATA PROTECTION?

Introduction

India introduced the Digital Personal Data Protection Act ('DPDPA') in the year 2023 to regulate how organizations handle personal data of their customers. The compliance obligations for organizations under DPDPA shall come into effect only from May 2027.

This marks a significant shift in how organisations handle personal data, because compliance is no longer a legal formality and it is directly linked to the credibility of the organization, customer trust, cyber resilience, and effective risk management.

This law affects all organizations in India, irrespective of their scale and size, as every organization today collects and handles digital personal data of employees, customers, vendors, and other stakeholders, such as name, address, mobile number, email ID, etc.

The timeline provided under DPDPA gives organizations sufficient time to ensure compliance with the provisions of DPDPA. Such compliance becomes vital as penalties for non-compliance range between INR 50 crores to 250 crores.

The Salient Features of DPDPA, 2023 have been discussed in detail in our ***Cyber Niyam Issue 1 of 2025.***

.....Continued on page 2

Why DPDPA compliance matters to you.

- **Builds third-party trust**: Fosters greater trust in the course of third parties, such as customers/vendors.
- **Protects the reputation of the organization**: Data leaks / Security breaches can damage your reputation.
- **Ensures legal compliance**: Compliance failures can result in penalties ranging from 50 to 250 crores
- **Benefits the organization from an operations perspective**: Organized data assists in managing the organization more efficiently

UNDERSTANDING YOUR DATA JOURNEY

Every organization handles digital personal data in multiple **stages**. From the moment you collect a Third Party's details until the time you finally delete them, the law expects you to act responsibly, transparently, and securely **at every stage** of this data journey.

Stage 1: You Collect It
Third Party personal data enters your organization when they provide details such as their name, phone number, address, email ID, payment information, or identity details in the course of dealings with the organization, such as purchase/supply of goods, rendering/availing services, or making enquiries, etc. You must collect only necessary information and clearly inform them about what is being collected and why.

Stage 2: You Store It
After collection, Third Party personal data shall be stored in various systems /databases of the organization, such as registers, billing systems, mobile devices, email inboxes, accounting software, or cloud-based systems. You are responsible for keeping this data organised, accurate, and accessible only to authorised persons.

Stage 3: You Use It
Third Party personal data is used for legitimate organizational purposes such as billing, rendering services, selling or purchasing goods, marketing, advertising, organizational procedures, delivery updates, service reminders, and permitted promotional communication. You must use the data only for the purposes disclosed to the Third Party.

Stage 4: You Protect It
You must protect customer data from loss, theft, unauthorised access, and misuse by using passwords, access controls, locked storage, and cybersecurity practices. Any data breach must be handled promptly and reported as required by law.

Stage 5: You Retain and Delete It
Customer data may be kept only for as long as required for organizational or legal purposes. Once the purpose is complete, you must safely delete or permanently erase the data.

GOOD TO KNOW!

What is the Data Protection Board?

The **Data Protection Board of India (DPB)** is the statutory authority responsible for the enforcement of the Digital Personal Data Protection Act, 2023. It was established by the Central Government under the DPDP Act, 2023, as India's primary digital data protection regulator to oversee lawful processing of personal data and safeguard the rights of individuals.

The Board's primary role is to ensure compliance with data protection obligations by Data Fiduciaries and Consent Managers, and to provide an effective grievance-redressal mechanism for individuals whose data protection rights are violated. It acts as the central authority for adjudicating complaints relating to personal data breaches and unlawful processing.

It conducts inquiries into data breaches and non-compliance, issues binding directions, accepts voluntary undertakings, and imposes monetary penalties for violations of the Act. It also directs urgent remedial and mitigation measures during data breach incidents.

The Board operates as a fully digital authority, conducting complaints, hearings and decisions through online systems. It strengthens India's data protection regime by enforcing privacy rights and promoting transparent and accountable data governance.

COLLECTION

Collection of private data means obtaining personal information from individuals, such as their name, phone number, address, or email, for providing goods or services. The organization must clearly inform the person why the data is being collected and obtain their consent before using it.

RETENTION

Retention means keeping personal data in your records after it has been collected. You may keep this data only for as long as it is required for the organization or legal purposes, after which it must be deleted.

SECURITY

Security means protecting personal data from loss, misuse, unauthorized access, and cyber-attacks. Organizations must use reasonable safeguards such as passwords, restricted access, and secure systems to keep data safe.

MODIFICATION/ERASURE

Modification and erasure refer to correcting, updating, or deleting personal data when requested by the individual. Organizations must make it easy for people to change wrong information or delete their data once it is no longer needed.

SHARING

Sharing means providing personal data to third parties such as delivery partners, payment processors, and service vendors. Date may be shared only for legitimate organizational purposes and with proper safeguards in place.

FREQUENTLY ASKED QUESTIONS

Practical Guidance on the Applicability and Implementation of the DPDP Act, 2023

The DPDPA lays down clear legal standards for how organizations must handle digital personal data. While the law applies to almost every organization that collects third party personal information, many organizations remain unsure about how these duties/compliances translate into everyday operations. This FAQ section answers common questions in simple language to help organizations understand their responsibilities, ensure compliance, and build customer trust through lawful data practices.

Q1. DO I HAVE TO TELL CUSTOMERS WHAT PERSONAL DATA I AM COLLECTING?

Yes. During the Collection stage of the data journey, the DPDPA requires organizations to be fully transparent with customers. Before collecting any personal information, third parties must be informed about what data is being taken, why is it collected, and how it will be retained and used.

- Consent for such data collection, retention, and usage must be obtained by issuance of a notice prior to collection. This notice for obtaining consent should be comprehensive, clear, and in simple language, thereby clarifying all aspects of the personal data journey.
- Only personal data that is genuinely required for organizational purposes should be collected, and unnecessary or excessive data must be avoided.

Q2. CAN I USE THIRD PARTY DATA FOR ANY OTHER PURPOSE LATER?

No. During the stage of use/processing of personal data, it can be used only for the purpose that was originally disclosed to the third party by means of the notice at the Collection stage. Using the data for any additional or new purpose without permission is treated as unlawful processing.

- If the organization wants to use the personal data for sharing with third parties, marketing,, or analytics, fresh consent must be obtained.
- Any unauthorized use can expose the organization to regulatory action and heavy penalties.

Q3. HOW LONG CAN I KEEP PERSONAL INFORMATION?

At the stage of retention of personal data, organizations may keep personal data only for as long as it is required to fulfil the legitimate needs outlined in the notice. Retention must always be linked to a clear organizational or legal purpose.

- Data must be securely deleted once the stated purpose has been achieved.
- Storing data indefinitely or "just in case" is not allowed under the DPDPA.

Q4. CAN I SHARE PERSONAL INFORMATION WITH THIRD PARTIES?

Yes, but carefully. Personal data may be shared only with trusted service providers/vendors such as IT service providers, sub-contractors, payment gateways, cloud service providers, accountants, third party professionals and only for genuine organizational purposes.

- The organization remains legally responsible for how third party service providers use and protect third party data.
- Vendors must be contractually bound to use personal data only for agreed purposes and maintain proper security safeguards.

Q5. DO I NEED TO UPDATE MY EXISTING VENDOR/SERVICE PROVIDER AGREEMENTS?

Yes. Organizations must update their agreements to include data protection clauses. These clauses ensure that vendors/service providers are legally bound to protect personal data.

- Contracts must specify confidentiality duties, security measures, and limits on data usage.
- Vendors/service providers must follow the same or higher security standards as your organization.

Q6. HOW SHOULD I PROTECT THE PERSONAL DATA?

The DPDPA requires organizations to implement reasonable technical and organizational safeguards to prevent data leaks, hacking, loss, or misuse.

- Measures should include passwords, restricted access, secure devices, and regularly updated systems.
- Serious cyber incidents must be promptly reported to CERT-In and the Data Protection Board of India.

Q7. SHOULD MY STAFF BE TRAINED ON DATA PROTECTION?

Yes. Staff training becomes critical because employees directly handle personal data in daily operations.

- Employees must be trained on safe data handling and breach response procedures. Such training must be provided regularly.
- Written internal policies, such as Data Protection policy (which is separate from Information Security policy), FAQs, and escalation processes must be available.

Q8. HOW SHOULD I HANDLE CHILDREN'S PERSONAL DATA?

Under the DPDPA, processing personal data of individuals under 18 years of age requires strict adherence to safety standards and parental oversight. Organizations must transition from standard data practices to a protected framework to ensure the digital well-being of minors.

- **Verifiable Consent:** You must obtain prior, verifiable consent from a parent or lawful guardian before any processing begins.
- **Harm Prevention:** Any data processing likely to cause a detrimental effect on a child's physical or mental well-being is strictly prohibited.
- **No Profiling:** You are barred from tracking, behavioral monitoring, or directing targeted advertising toward children.
- **Accuracy Duties:** You must ensure children's data is complete and accurate, especially if used to make decisions affecting them.

Q9. HOW DO I KNOW IF I AM A SIGNIFICANT DATA FIDUCIARY?

DPDPA provides that the Government may notify certain large or high-risk organizations as Significant Data Fiduciaries based on the volume and sensitivity of data handled.

- Such organizations must appoint a Data Protection Officer and conduct regular audits.
- They must also carry out Data Protection Impact Assessments and maintain stricter compliance.

However, currently, no organizations have been named as Significant Data Fiduciaries yet.
In our view, organizations that handle significant volumes of personal data, such as educational institutions, hospitals (handling sensitive medical information), social media companies, and e-commerce platforms, shall qualify as Significant Data Fiduciaries.

Q10. WHAT PENALTIES APPLY FOR NON-COMPLIANCE?

The DPDPA replaces traditional criminal imprisonment with a significant civil penalty regime designed to ensure that data protection is treated as a core business priority rather than a mere formality.

- **Corporate Deterrence (Up to ₹250 Crore):** To ensure large-scale data security, the Act sets massive ceilings specifically ₹250 crore for failing to prevent data breaches and ₹200 crore for violating child safety norms to make non-compliance more expensive than the cost of implementing security.
- **Graded Adjudication:** The Data Protection Board does not apply a "one size fits all" fine; it must consider the nature, gravity, and duration of the breach, the repetitive nature of the offense, and whether the entity realized a financial gain from the lapse.

NEXT STEPS
Steps to be taken by organizations to ensure compliance

IMPLEMENT A TRANSPARENT NOTICE MECHANISM FOR THE COLLECTION OF PERSONAL DATA.

ESTABLISH AN EFFECTIVE DATA MODIFICATION AND CORRECTION MECHANISM.

STRENGTHEN CYBERSECURITY MEASURES (TECHNICAL AND ORGANISATIONAL).

IMPLEMENT A DATA BREACH IDENTIFICATION AND NOTIFICATION MECHANISM.

CONDUCT REGULAR EMPLOYEE TRAINING AND AWARENESS PROGRAMS.

REVIEW AND UPDATE AGREEMENTS WITH THIRD PARTY VENDORS HANDLING PERSONAL DATA.

DRAFT AND IMPLEMENT A DATA PRIVACY POLICY

GLOSSARY OF TERMS

What is Personal Data?

Under India's **Digital Personal Data Protection (DPDP) Act, 2023,** and the newly notified **2025 Rules**, **Personal Data** is any data about an individual who is identifiable by or in relation to such data. Essentially, if a piece of information or a combination of different pieces of information can be used to figure out exactly who a person is, it qualifies as personal data. The law specifically focuses on **Digital Personal Data**, meaning it covers information that is either collected directly in digital form (like on a website) or collected on paper and later scanned or entered into a computer.

To help you identify it in your organization or daily life, here are common categories:

1. **Direct Identifiers:** Your full name, home address, personal email ID, and mobile number.
2. **Government Identifiers:** Aadhaar number, PAN card details, Passport number, or Voter ID.
3. **Digital Footprints:** IP addresses, GPS location data, device IDs, and browser cookies that track your online behavior.
4. **Biometric Data:** Fingerprints, facial recognition data, or voiceprints used for attendance or security.
5. **Financial & Health Records:** Bank account statements, transaction history, medical prescriptions, and insurance details.

In short, "Personal Data" acts as a digital bridge between a piece of information and a real human being. Because this data is so closely tied to your identity, the law now mandates that companies (Data Fiduciaries) cannot use it without your clear permission, must keep it secure from hackers, and are legally required to delete it once it is no longer needed for the specific reason it was collected.

What is a Data Fiduciary?

A **Data Fiduciary** is the entity (such as a company, shop, or online platform) that decides **why** and **how** your personal data is collected and used. Under India's DPDP Act, they are viewed as "trustees" of your information, meaning they are legally responsible for keeping it safe, getting your clear consent, and deleting it once the purpose is served. Even if they hire a third party to process the data, the Data Fiduciary remains the one held accountable by law for any breaches or misuse.

What is a Data Principal?

A Data Principal is the individual to whom personal data relates, and under the DPDP Act 2023, you are granted specific rights to ensure you remain the primary authority over your digital information. This legislation empowers you to demand a summary of your processed data, correct inaccuracies, and request the total erasure of your information once its purpose is served or consent is withdrawn. You also have the right to nominate a representative to manage your data in case of death or incapacity and must be provided with an accessible grievance redressal mechanism by any organization handling your data. However, these rights are balanced by a set of legally binding duties intended to prevent misuse of the law and maintain the integrity of the digital ecosystem. As a Data Principal, you are required to furnish only verifiably authentic information, avoid impersonating others, and refrain from filing false or frivolous complaints with the Data Protection Board. To ensure responsible participation, the Act prescribes a penalty of up to ₹10,000 for individuals who fail to perform these duties, emphasizing that data privacy in India is a collaborative responsibility between citizens and organizations.

NEWS CORNER

Constitution of the Data Protection Board (DPB)

The Indian government has accelerated the formal establishment of the Data Protection Board (DPB), a pivotal independent body tasked with enforcing the nation's new digital privacy standards. To ensure a "digital-first" approach, the Ministry of Electronics and IT (MeitY) has already developed a specialized software ecosystem, including a portal and mobile app, allowing the Board to function as a paperless office where citizens can file and track complaints in real-time. Currently, the government has finalized the appointment process for a four-member board, including a Chairperson, through high-level search and selection committees. Once fully operational, the Board will have the power of a civil court to summon witnesses, inspect data records, and investigate breaches, with the authority to impose heavy penalties of up to ₹250 crore for severe compliance failures.

NEWS CORNER

Implementation of DPDP Rules

On 14 November 2025, the government officially notified the Digital Personal Data Protection (DPDP) Rules, providing the essential procedural "blueprint" for how the 2023 Act will be implemented by organizations and government agencies. These rules introduce the "SARAL" approach—Simple, Accessible, Rational, and Actionable, which mandates that companies use plain, non-technical language and illustrations in their consent notices to ensure users truly understand how their data is being used. One of the most significant provisions is the strict 72-hour timeline for reporting personal data breaches to the Board, ensuring that incidents are no longer hidden from affected individuals. The rules also grant organizations a phased 18-month compliance window to overhaul their internal technical systems, particularly for implementing "Data Erasure" protocols that require deleting inactive user data after three years, preceded by a mandatory 48-hour warning. Furthermore, the framework establishes "Consent Managers," which are Indian-registered entities that will serve as a single dashboard for citizens to manage, review, and withdraw their data permissions across multiple apps and websites. By clarifying these granular requirements, the 2025 Rules transform the privacy law into an enforceable reality, balancing the rights of "Data Principals" with the operational needs of "Data Fiduciaries."

ABOUT THE AUTHORS

Adv Vaishali Bhagwat

Vaishali Bhagwat is a practicing lawyer with 25 years of experience in civil and cyber litigation and advisory practice in Pune and Mumbai.
Vaishali has a prior degree and work experience in the field of Computer Science, a Post graduation certification in Cyber Security and Information Assurance and is a certified Privacy Lead Assessor.

She is an advisor to several companies on Cyber law and privacy compliance and advisor to various educational institutions on Protection of children from sexual offences.

She has successfully conducted several prominent cases for corporate espionage and Data theft, Data Privacy, Digital Financial Frauds, Cyber-crimes against women and children, take down orders and IP infringement in cyberspace.

Vaishali is a *TCS Chevening Scholar on "Cyber Policy and Cyber Defense" and has earned the Post Graduate certification from Cranfield University UK. She is also a Disha Alumni which is a prestigious program of the British high Commission on Innovative Leadership chaired by UK PM David Cameron and PM Manmohan Singh*.

www.vaishalibhagwat.com

Adv Kunal Gokhale
BSC. LLB (Hons.) (Business Law) Degree

Advocate Kunal Gokhale is a legal professional with nearly fourteen years of post-qualification experience. He is a graduate from the National Law University, Jodhpur and holds a BSc LLB (Hons.) (Business Laws) degree. Advocate Kunal Gokhale has significant professional experience in handling civil litigation matters with focus on commercial matters. He also provides advisory services in relation to drafting of various types of agreements and has been associated with firms such as Vaish Associates, Advocates (Delhi), Ernst & Young, India (Mumbai) and Luthra & Luthra Law Offices (Mumbai) in the past.

Mrudula Arjunwadkar
BSc., LLB, MPM

POSH Consultant
Helping organizations in end to end POSH Compliance, External member to IC, POSH trainings