© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1720115

Digital Personal Data Protection Act, 2023

BHAVYA
Uttaranchal University

Abstract- ***The Digital Personal Data Protection Act marks a significant transformation in India's privacy and data governance framework. While most discussions focus on consumer privacy and technology companies, the Act's impact on employee data management remains underexplored. Every organisation processes large volumes of employees' personal data during recruitment, onboarding, payroll administration, performance evaluation, disciplinary proceedings, and post-employment activities. This paper examines the obligation imposed by the DPDP Act on employers and proposes a corporate employees' data governance framework for ensuring compliance, reducing legal risk, and strengthening organisational trust.***

Keywords: Digital Personal Data Protection Act, Employee Privacy, Data Governance, Data Fiduciary, Data Principal, Human Resources, Corporate Governance, Data Protection.

I. INTRODUCTION

Data has become one of the most valuable assets for modern organisations. Employers routinely collect personal information such as identity documents, educational records, bank account details, tax records and performance assessments. The DPDP Act establishes a comprehensive legal framework governing the collection, processing, storage, transfer and deletion of digital personal data. The Act recognises the individual whose data is processed as a data principal and the organisation determining the purpose and means of processing as a data fiduciary. Consequently, employers become data fiduciaries, and employees become data principals.

The Draft Rules are characterised by simplicity and clarity in language, making them accessible to a wide audience. Below are the key highlights:

- Form of notice

The Draft Rules mandate that any notice issued to data principals by data fiduciaries must be independently understandable without reliance on additional information. This ensures transparency and comprehensibility, promoting trust and informed consent.

- Consent managers

The DPDP Act has introduced the concept of consent managers. The Draft Rules now outline their eligibility criteria and obligations. A consent manager must be an entity incorporated in India with a minimum net worth of INR 2,00,00,000 (approximately USD 240,000). Additionally, they are required to demonstrate technical, financial, and operational capacity. The Draft Rules emphasise sound financial health and general character, though these requirements remain broadly defined. It will be clearer if specific quantifiable benchmarks are incorporated to eliminate ambiguity, which will ensure uniform compliance.

- Reasonable security safeguards

The data fiduciaries and processors are obligated to implement reasonable security measures, such as encryption and obfuscation, to protect personal data. They must maintain visibility over data access through appropriate logs and monitoring mechanisms, enabling detection, investigation, remediation of unauthorised access, and measures to prevent recurrence.

- Intimation of data breach

The DPDP Act mandates data breach notifications to data principals. The Draft Rules, however, lack differentiation among breaches based on severity, nature of data, or impact. Categorising breaches and introducing quantitative thresholds for notification would alleviate unnecessary burdens on the data fiduciary and save the data principals from constant intimations, while ensuring timely intimation of critical incidents.

- Retention and erasure

© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1720115

The Draft Rules introduce data retention timelines for specific fiduciary classes (for instance, an e-commerce entity having not less than 2 crore users in India is required to retain personal data for three years from the date which the data principal last approached them for the performance of the specified purpose or exercise of her rights, or the commencement of the Draft Rules whichever is latest) and require them to notify data principals 48 hours prior to data erasure if the specified purpose is unfulfilled or rights remain unexercised. However, it will be helpful if more clarity is provided on retention obligations for data fiduciaries not listed in the Third Schedule. Comprehensive guidance would aid in consistent adherence across sectors.

- Verifiable consent for children's data and persons with disability

The Draft Rules detail processes for obtaining verifiable parental consent when processing children's personal data and personal data of persons with disabilities. This includes validating parental identity and age through reliable documents or digital locker tokens. Notably, the Explanatory Statement to the Draft Rules requires fiduciaries to confirm the parent-child relationship, a potentially onerous task. Further clarification on the extent of fiduciary diligence in such cases is imperative to avoid operational challenges. Additionally, the Draft Rules also now provide clarity on what constitutes a “person with disability” under the Rights of Persons with Disabilities Act, 20162andNational Trust for Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Act, 19993.

- Obligations of significant data fiduciaries

The DPDP Act had introduced the concept of significant data fiduciaries (SDFs) to be determined on the basis of factors such as data volume, sensitivity, and potential risks to democracy and individual rights. While the Draft Rules state that SDFs must conduct annual audits and data protection impact assessments (DPIAs), they do not prescribe a format or manner of conducting such DPIAs. Further, while the DPDP Act provides the factors for determination of an SDF, the Draft Rules do not shed any further clarity on the classification based on those factors. The classification will be helpful for determining whether operations/businesses will be classified as an SDF or an entire entity (which could be in multiple businesses) will be classified as an SDF.

- Rights of data principals

The Draft Rules elaborate on the role of consent managers in enabling data principals to exercise their rights. They also specify the information consent managers must publish to facilitate the exercise of these rights, ensuring transparency and accessibility.

II. LEGAL FRAMEWORK UNDER THE DPDP ACT

Obligations of Data Fiduciary

• Broadly, the proposed obligations of the Data Fiduciary will include implementation of technical and organisational measures for compliance, security safeguards to prevent data breach, intimation of data breaches to affected Data Principals and the Data Protection Board, erasure of data upon withdrawal of consent or when retention is no longer necessary for the specified purpose, publishing of contact details of person to answer queries of Data Principals, establishing of a grievance redressal system, and use of Data Processors only under contract.

• Further, certain additional obligations are proposed in respect of Data Fiduciaries notified as Significant Data Fiduciaries, such as appointing a data auditor and conducting periodic Data Protection Impact Assessments to ensure a higher degree of data protection.

Additional obligation

- Appointment of data protection officer
- Appointment of an independent data auditor
- Periodic data protection impact assessments
- Regular compliance audits
- Enhanced governance and accountability mechanisms

1.Need for Appointment of a Data Protection Officer (DPO)

Acts as the contact person between the company, data principals (individuals), and the government.

Handles complaints and grievances related to personal data.

Monitors compliance with the DPDP Act and company policies.

Helps reduce the risk of data breaches and legal penalties.

2. Need for Appointment of an Independent Data Auditor
Provides an unbiased assessment of the company's data protection practices.

Verifies whether the company complies with legal requirements.

Identifies weaknesses in data security and governance.

Builds trust among customers, investors, and regulators.

3. Need for Periodic Data Protection Impact Assessment (DPIA)
Evaluates risks before or during data processing activities.

Identifies potential harm to individuals' privacy.
Helps organisations implement safeguards to reduce risks.

Demonstrates proactive compliance with the DPDP Act.

4. Need for Regular Compliance Audits
Ensures that data protection policies are effectively implemented.

Detects non-compliance and security gaps at an early stage.

Helps organisations avoid penalties and reputational damage.

Encourages continuous improvement in data management practices.

5. Need for Enhanced Governance and Accountability Mechanisms
Establishes clear responsibilities for data protection within the organisation.

Ensures senior management oversight of privacy practices.

Creates a culture of accountability and transparency.
Improves stakeholder confidence and corporate reputation.

Supports effective response to data breaches and regulatory inquiries.

Employee rights

- Right to access personal data
- Right to correction and updating
- Right to erasure
- Right to nominate another person in case of death or incapacity
- Right to give or Refuse Consent Data Protection Board of India

The DPBI serve as the central regulatory authority under this act Function.

- Monitor compliance
- Investigate complaints
- Adjudicate violations
- Impose penalties
- Direct remedial measures
- Oversee consent managers. Proposed corporate employee data governance framework
- Data mapping and classification: - organisation should create an employee data inventory categorising data into basic personal data, financial data, biometric data, health data,

Penalties Under the DPDP Act, 2023
The DPDP Act imposes substantial financial penalties for non-compliance by Data Fiduciaries. The highest penalty up to ₹250 crore applies to failure of a Data Fiduciary to maintain reasonable security safeguards. Not notifying the Board or affected individuals of a personal data breach, as well as violations of obligations relating to children, can

each attract penalties of up to ₹200 crore. Any other violation of the Act or Rules by a Data Fiduciary may attract penalties up to ₹50 crore.

Time periods

• Complaint to data fiduciary: - The Act requires a data principal to first approach the data fiduciary through its grievance redressal mechanism. The exact response period is to be prescribed by rule under section 13(2).

• Complaint before the data protection board: - After exhausting the grievance redressal process, the data principal may file a complaint before the DPBI.

• Appeal against board order: - Any person aggrieved by an order or direction of the board may file an appeal before the appellate tribunal within 60days from the date of receipt of the order

• Disposal of appeal: - the appellate tribunal should endeavour to dispose of the appeal within 6 months from the date of filing

• Voluntary undertaking: - submitted at any stage of proceedings before the board

Note: - organisations have approximately 18 months to achieve full compliance with all substantive provisions of the Act, including consent management, security safeguards, data subject rights, and grievance redressal mechanisms

Benefits of the 18-month compliance window for companies

- Reduces the likelihood of widespread non-compliance when the law becomes enforceable
- Helps organisations align contracts, policies and internal procedures with statutory requirements
- Enables businesses to train employees and implement technical safeguards
- Strengthens protection of personal data by ensuring compliance measures are properly established before strict enforcement begins.

III. KEY IMPLEMENTATION DATE: -

- NOVEMBER 2022: Digital Personal Data Protection Bill introduced
- AUGUST 2023: Digital Personal Data Protection Act passed by Parliament
- 11 AUGUST 2023: Presidential assent received, and DPDP became law
- 13 NOV 2025: Notification establishing the Data Protection Board of India and regulatory infrastructure
- 13 NOV 2026: Consent manager framework activation
- 13 MAY 2027: Full compliance obligation and enforcement

IV. FUNCTIONS OF THE BOARD

The Data Protection Board has been vested with mainly adjudicative functions. The Board has been set up with the objective of ensuring that the data fiduciaries and data principals are in compliance with the provisions of the Bill and has been given the power to conduct inquiries, summon witnesses, examine evidence, carry out proceedings with respect to the complaints received and levy penalties. Given the expansive range of powers of the Board, it is important to get its composition right such that it functions independently of the influence of the Central Government.

Under this Act, an employer may be required to give access to a third party to an employee's personal data if such employee nominates such party to exercise the employee's rights under the Act upon their death or incapacity. employee could nominate any third party to access,

While conducting internal investigations/disciplinary proceedings, certain employers transfer a significant amount of personal data to an investigation agency outside India. In such cases, employers will be required to comply with this Act.

As immediate steps, employers should consider appointing a team that will be responsible formulating/revising the relevant policies and implementing the necessary procedures and

protocols, identifying gaps and ensuring compliance with this Act. Employers are also engaging external service providers with specific expertise to guide the internal team with the harmonisation process. Further, if an employer has outsourced a few of its employee-related operations and shared employees' personal data with such third parties, it is crucial for employers to revisit the contracts with such third parties to ensure that there are adequate data protection clauses in the agreement in the context of this Act.

While the Act is a step in the right direction, it entails significant preparation on the part of an employer before the legislation is brought into effect.

The Government of India released some guidelines on the governance of AI tools.

The Guidelines are released in 4 parts:
Part 1 sets out the seven sutras that ground India's AI governance philosophy.

The sutras of Trust, People First, Innovation over Restraint, Fairness & Equity, Accountability, Understandable by Design and Safety, Resilience & Sustainability are designed to be technology-agnostic and applicable across all sectors.

Part 2 examines key issues and offers recommendations through six pillars across three key domains: enablement (infrastructure, capacity building), regulation (policy & regulation, risk mitigation) and oversight (accountability, institutions).

Part 3 presents an action plan outlining short, medium, and long-term steps to operationalise these recommendations through a whole-of-government approach leveraging the Technology & Policy Expert Committee and AI Governance Group for strategic oversight, and the AI Safety Institute for technical validation & safety research.

Part 4 provides practical guidelines for industry actors and regulators to ensure consistent and responsible implementation of the recommendations.

India has developed a pragmatic approach to AI governance that is emphasised by a techno-legal framework supported by voluntary measures and Digital Public Infrastructure (DPI). The future of India's leadership in this revolution depends on our ability to lead by example in governing this technology with foresight, ensuring it remains safe, inclusive, and a force for global good.

Under section 8, the most relevant provision for using AI by companies because the companies remain accountable for personal data processed through AI systems, whether the AI is developed internally or provided by a third party.

V. POLICY ON THE USE OF ARTIFICIAL INTELLIGENCE IN JUDICIAL AND COURT ADMINISTRATION

CONFIDENTIALITY AND DATA PROTECTION
General Rule: No confidential information or data shall be entered into any public AI tool.
Public AI Tools: Where a public AI tool (e.g., the free tier of any LLM) is being used, no Court Documents — unless otherwise publicly available — and no case-related information shall be entered as prompts or context. Use of public AI tools shall be restricted to general, non-case-specific research and administrative tasks only.

Enterprise/Private AI Tools: In cases where the High Court of Gujarat approves an enterprise or private AI deployment under a formal data processing agreement that prohibits the provider from using inputs for model training or third-party disclosure, such tools may be used for a wider range of tasks as specified in Clause 7. However, the following shall continue to be prohibited even in enterprise deployments: • Entry of witness identities in pending criminal matters. • Entry of information subject to confidentiality orders passed by any Court. • Biometric, health, or other Special Category Personal Data as defined under the Digital Personal Data Protection Act, 2023.

Compliance with DPDP Act, 2023: All AI-related data processing involving personal data shall comply with the Digital Personal Data Protection Act, 2023

and rules made thereunder as and when it comes into force. Users shall not use AI tools to process personal data for purposes beyond those for which such data was originally collected during judicial proceedings.

VI. PROHIBITED USES OF AI TOOLS

Notwithstanding any other provision of this Policy, the following uses of AI are absolutely prohibited:

1. Artificial intelligence shall never be employed for any form of decision-making, judicial reasoning, order drafting, judgment preparation, bail/sentencing considerations, or any substantive adjudicatory process. Broadly, Artificial intelligence shall not be 8 HIGH COURT OF GUJARAT | Policy on Use of Artificial Intelligence used—directly or indirectly—for any aspect of judicial decision, adjudication, reasoning, application of law, interpretation of facts, weighing of arguments, determination of rights/liabilities, sentencing, bail, interim orders, or final judgment.
2. Using AI to arrive at, determine, or substantially influence any finding of fact, finding of law, or operative order in any judicial proceeding.
3. Artificial intelligence shall not be used for sorting evidence, classification of evidence, organisation of evidentiary material, credibility assessment, relevance filtering, summarisation of depositions/testimony, or any task involving evaluation or categorisation of proof.
4. Using AI to author, generate, or substantially compose any judgment, final order, or binding legal ruling, even if subsequently reviewed by a judge.
5. Entering any of the following categories of information into any public AI tool:

5.1 Names, addresses, or identifying information of parties, witnesses, or advocates;

5.2 Details of pending proceedings or unreported orders;

5.3 Privileged communications or confidential legal strategies;

5.4 Sensitive personal data as defined under the DPDP Act, 2023 (including health, financial, biometric, or caste-related information);

5.5 Evidence or documents filed in a case.

6. Using AI to generate, fabricate, embellish, or alter evidence in any form.
7. Using AI-generated citations, case references, or statutory provisions without independent verification from authoritative primary sources such as AIJEL, SCC Online, AIR, the Supreme Court website, or official government gazettes. 8. Sharing AI-generated content that mimics or purports to represent the official reasoning or language of a judge without the judge's authorisation.
8. AI Tool shall not be used for the purpose of drafting, correcting or summarising any office note or submission.
9. Accessing AI tools using Court credentials on personal devices in a manner that bypasses security protocols established by the High Court.
10. Using AI for any purpose that violates any provision of the laws and rules

VII. CONSEQUENCES OF VIOLATION

Violation of any provision of this Policy shall be treated as misconduct and shall attract appropriate action including departmental or disciplinary proceedings under applicable service rules. The above consequences are in addition to, and not in derogation of, any civil or criminal liability that may arise under any applicable law, including the Information Technology Act, 2000, the DPDP Act, 2023, or the Bharatiya Nyaya Sanhita, 2023

Source- OECD Best Practice Principles for the Governance of Regulators (OECD, 2014)

Considering the OECD Guidelines on independence of regulators, the independence of the Data Protection Board envisaged under the PDP Bill, 2022 needs to be determined in terms of the composition, structure, appointment process and functions of the Board. An assessment of the quasi-legislative, quasi-executive and quasi-judicial functions of the Board will be undertaken to analyse the independence, accountability and transparency of the Board. Further, the article will compare these with the structure and functions of the DPA laid down under the PDP Bill, 2019 to see if the regulatory structure has evolved.

© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1720115

In the cases of Rojer Mathew south bank and S.P. Sampath Kumar v. U.O.I where the courts held that selection committees to quasi-judicial bodies must compulsorily have a judicial member. This has been regarded as necessary to safeguard the independence and impartiality of the tribunal since the government could be the litigant in many cases; hence, the need to separate any bias from the adjudication process.

Difference between India-DPDP and EU-AI Act

Aspect	India -DPDP Framework	EU - AI Act Framework
Regulatory Nature	Principle-based, data protection-oriented	Risk-based, AI-specific regulation
Scope	Focus on personal data processing	Covers AI systems across risk categories
Bias Mitigation	Indirect, through fairness and data accuracy obligations	Direct, with mandatory safeguards for high-risk AI
Risk Classification	Absent	Clearly defined categories
Transparency	General obligations	Specific disclosure and explainability requirements
Accountability	Data Protection Board of India	National and EU-level supervisory authorities
Enforcement	Emerging framework	Strong penalties and compliance mechanisms
Algorithmic Audits	Not expressly mandated	Mandatory for high-risk systems
Fundamental Rights	Implicit protection	Explicit integration

Minor differences between DPDP AND GDPR

BASIS	DPDP ACT	GDPR ACT
Scope	Cover digital personal data	Covers both digital and non-digital personal data.
Legal basis	Primarily based on consent and certain legitimate uses.	Provides multiple legal bases such as consent contract legal obligation legitimate interests etc.
Data protection officer	Mandatory mainly for significant data fiduciaries	Mandatory in specified cases involving public authorities or large-scale processing
Data auditor	Requires independent data auditors for significant data fiduciaries.	No specific concept of mandatory data auditor
Children data	Age threshold generally below 18 years	Usually below 16 years (member states may reduce it to 13 year)
Data breach notification	Notification to the data protection board and affected individuals as prescribed.	Notification to supervisory authority within 72 hours of becoming aware of the breach
Regulatory authority	Data protection board of India	Independent supervisory authorities in each EU member state.

Penalties	Monetary penalties up to 250 crores for certain violation.	Administrative fines 20million or 4% of global annual turnover whichever is higher
Right to data portability	Not expressly provided	Expressly recognized under article 20 GDPR
Right to be forgotten	Limited rights through erasure and grievance mechanisms	Explicit right to erasure under article 17

FOR EXAMPLE: Collection of personal data across departments.

In a modern organisation, personal data is collected by multiple departments for different business purposes.

A company may have some of these departments that collect information directly and indirectly. Therefore, compliance with the Digital Personal Data Protection Act 2023 requires coordination among all departments handling personal data to ensure lawful collection, storage, processing and protection of such information.

DEPARTMENT	TYPES OF PERSONAL DATA INFORMATION COLLECTED BY THE COMPANY
(HR) Human resource	Employee records, Aadhaar card, pan card, salary detail, passbook, marksheet
Marketing	Customer name, mobile number, email id, address
Sales	Contact details, purchase history,
Finance	Bank details, tax information
IT	Login credential, IP addresses, system logs
Administration	Employees contact details, emergency contact information, visitor record and entry registers, identity card information, office access and attendance record, vehicle registration details for parking management, CCTV footage and security related records.