Vol 6, Issue 7, July 2026 www.ijesti.com E-ISSN: 2582-9734
International Journal of Engineering, Science, Technology and Innovation (IJESTI)

Implementation of The Digital Personal Data Protection Act, 2023: Challenges and Prospects in Jharkhand

Dr. Sachin Indiwar
Assistant Professor, Department of Law, Dr. Shyama Prasad Mukherjee University, Ranchi.
Corresponding Author: sachin.indiwar@gmail.com

ABSTRACT

The Digital Personal Data Protection Act, 2023 marks India's shift from sectoral privacy rules to a general framework for digital personal data. Its practical significance for Jharkhand lies primarily in public administration: certificates, pensions, scholarships, ration services, land records, health systems, education databases, policing and financial management routinely process identity, socioeconomic and sometimes sensitive contextual information. It argues that Jharkhand's principal challenge is not the absence of technology but the conversion of fragmented e-governance systems into an accountable data lifecycle. Legacy records, unclear departmental ownership, vendor dependence, limited breach readiness, multilingual and low-literacy interfaces, assisted access through service centres, children's data and the interaction between privacy and transparency create distinctive implementation risks. At the same time, the transition period offers a practical opportunity to build interoperable governance: statewide data inventories, purpose and retention registers, model notices, processor clauses, role-based access, incident playbooks, accessible grievance channels and independent audits. The paper proposes a tiered state implementation model that preserves service delivery while making necessity, security and citizen control demonstrable.

Keywords: *Digital Personal Data Protection Act; DPDP Rules; Privacy; Data Fiduciary; Jharkhand; E-Governance; Personal Data Breach; Digital Inclusion.*

I. INTRODUCTION

The right to privacy is protected as an intrinsic part of life and personal liberty under article 21 of the Constitution. In Justice K.S. Puttaswamy (Retd.) v. Union of India, the Supreme Court described informational privacy as a constitutional concern and required restrictions on privacy to satisfy legality, legitimate aim and proportionality. The Digital Personal Data Protection Act, 2023 (DPDP Act) translates part of that constitutional obligation into a horizontal statutory framework for processing digital personal data. It applies to data collected digitally and to non-digital personal data subsequently digitised; its reach can extend outside India where processing is connected with offering goods or services to Data Principals in India.12

For Jharkhand, implementation is inseparable from e-governance. JharSewa alone integrates applications for birth, caste, income and residence certificates, social-security pensions, revenue services, ration-card functions and other citizen services, including assisted delivery through Common Service Centres or Pragya Kendras. The State portal also links land, food-distribution, registration, health, tax and geospatial systems. These services convert identity, family, disability, caste, income, location and benefit records into persistent digital trails. The DPDP question is therefore not whether the State may use data, but whether each use is lawful, necessary, secure, explainable and contestable.34

1 The Digital Personal Data Protection Act, 2023, Act No. 22 of 2023, long title and ss. 3–4.
2 Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
3 Government of Jharkhand, Jharkhand State Portal, available at: https://www.jharkhand.gov.in/ (last visited July 22, 2026).
4 Government of Jharkhand, JharSewa, 'About Us' and service catalogue, available at: https://jharsewa.jharkhand.gov.in/ (last visited July 22, 2026).

This paper is a focused doctrinal and policy review. It analyses the Act, the final Rules, commencement notifications, constitutional cases, central cybersecurity instruments, Jharkhand's official service architecture and a recent CAG information-systems audit. The review is evaluative rather than empirical: it identifies legally material implementation gaps and proposes a staged compliance model without claiming to measure every state database or department.

II. THE PRESENT LEGAL POSITION

A. Phased Commencement

The Act received presidential assent on 11 August 2023, but it did not commence in full on that date. On 13 November 2025, the Central Government brought definitions, the institutional provisions concerning the Data Protection Board of India and selected miscellaneous provisions into force. The Consent Manager provision is scheduled one year after that date, while the principal provisions on processing, Data Fiduciary duties, Data Principal rights, adjudication and penalties are scheduled eighteen months after it.56

The Digital Personal Data Protection Rules, 2025 follow the same sequence: rules 1, 2 and 17–21 commenced on publication; rule 4 is scheduled after one year; and rules 3, 5–16, 22 and 23 after eighteen months. Consequently, as on 22 July 2026, Jharkhand is in a legally significant preparation window. The Board has been established in law and its appointment and digital-office architecture are notified, yet the Ministry's 2026 public material still advertised filling the posts of Chairperson and Members. The State should not present future core duties as already enforceable, but waiting until May 2027 would make credible compliance unlikely.78

Figure 1: Phased Commencement of The DPDP Act and Rules

Note. Dates follow the Gazette notification of 13 November 2025; the MeitY document page was posted on 14 November 2025.

5 Ministry of Electronics and Information Technology, Notification G.S.R. 843(E), Gazette of India, Extraordinary, Part II, s. 3(i), Nov. 13, 2025; India Code, commencement note to s. 1 of the DPDP Act.

6 The Digital Personal Data Protection Act, 2023, s. 1(2).

7 Ministry of Electronics and Information Technology, 'Filling up the post of Chairman & Members in the Data Protection Board of India (DPBI)', What's New, available at: https://www.meity.gov.in/whats-new (last visited July 22, 2026).

8 Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), r. 1(2)–(4).

B. Core Compliance Architecture

The Act permits processing for a lawful purpose on the basis of consent or certain legitimate uses. Consent must be free, specific, informed, unconditional and unambiguous, with clear affirmative action and an effective route to withdrawal. This does not mean that every government service requires consent. Section 7 permits defined legitimate uses, including voluntary provision for a specified purpose and processing by the State for specified benefits or functions, while rule 5 and the Second Schedule prescribe standards for public subsidies, benefits, services, certificates, licences and permits. The State must therefore document the correct legal basis instead of placing a generic consent checkbox on every form.910

A Data Fiduciary determines the purpose and means of processing and remains responsible for processing undertaken by a Data Processor on its behalf. Its central duties include accuracy where data affect decisions or disclosure, reasonable security safeguards, breach intimation, erasure when purpose and retention end, publication of a contact point and grievance redressal. The Rules specify protective measures such as encryption or masking, access controls, logs, backup and organisational controls; appropriate processor contracts; notification of affected Data Principals without delay; and an initial Board intimation followed by more detailed information within seventy-two hours, unless extended.1112

Data Principals receive rights of access, correction and erasure, grievance redressal and nomination, but also have duties against impersonation, suppression of material information and frivolous complaints. Children's processing is subject to verifiable parental consent and restrictions on tracking, behavioural monitoring and targeted advertising, subject to statutory and rule-based exceptions. Significant Data Fiduciaries face additional obligations, including an India-based Data Protection Officer, independent audit and periodic data-protection impact assessment.131415

Table 1: DPDP Obligations and Their Application to Jharkhand Government Systems

Legal Requirement	Jharkhand Application	Minimum Evidence
Purpose and legal basis	Map each field and data flow to statute, rule, scheme or valid consent	Processing register; approved purpose statement
Notice and citizen choice	Clear notice at portal, office and Pragya Kendra; withdrawal where consent applies	Versioned notices; language and accessibility testing
Accuracy	Higher control where certificates, benefits, employment, land or pensions are affected	Source, correction history and decision audit trail
Security and processors	Protect state, departmental, cloud and kiosk environments	Access matrix; logs; encryption; contracts; tests
Breach response	Coordinate department, JAP-IT/NIC, CERT-In, police and affected citizens	Playbook; incident register; notification records
Rights and grievances	One route across portals, with offline assistance and departmental ownership	Ticket, identity check, reasoned closure and appeal route
Retention and erasure	Reconcile DPDP limits with archives, finance, service and litigation requirements	Record schedule; holds; deletion certificate

9 Id., s. 7; Digital Personal Data Protection Rules, 2025, r. 5 and Second Schedule.
10 The Digital Personal Data Protection Act, 2023, ss. 4–7.
11 Digital Personal Data Protection Rules, 2025, rr. 6–7.
12 The Digital Personal Data Protection Act, 2023, s. 8.
13 The Digital Personal Data Protection Act, 2023, s. 10; Digital Personal Data Protection Rules, 2025, r. 13.
14 Id., s. 9; Digital Personal Data Protection Rules, 2025, rr. 10 and 12 and Fourth Schedule.
15 The Digital Personal Data Protection Act, 2023, ss. 11–15.

III. WHY IMPLEMENTATION IN JHARKHAND IS DISTINCTIVE

Jharkhand's service architecture combines statewide portals, departmental applications, centrally supported platforms, district offices and assisted-service intermediaries. A citizen may submit a document at a Pragya Kendra, have it processed in a district workflow, stored on shared infrastructure, verified against another database and used later for a benefit. Each handoff can create a processor, access-control, notice, retention and grievance question. The Department of Information Technology and e-Governance itself describes computerisation and electronic citizen-service delivery as a statewide governance objective.16

The recent CAG audit of Jharkhand's Integrated Financial Management System is instructive even though it was not a DPDP compliance audit. It found missing requirements documentation and data dictionaries, absence of a business-continuity plan, weak change management, inadequate helpdesk recording and application-control deficiencies. The audit also recorded direct production changes and deficiencies affecting data consistency and validation. These are precisely the governance conditions that can transform an ordinary software defect into inaccurate decision-making, unauthorised access or a reportable breach.1718

A second distinctive feature is inclusion. The Act permits notice in English or any language in the Eighth Schedule, and the Rules require clear and plain language. Formal availability in Hindi does not by itself ensure comprehension among citizens with limited literacy or speakers of Santali and other local languages. Assisted access can bridge that gap, but it also creates confidentiality risks when kiosk operators view identity and welfare documents. Privacy-by-design in Jharkhand must therefore include oral explanation, visual prompts, screened workstations, transaction receipts, operator accountability and a non-digital grievance route.19

IV. PRINCIPAL IMPLEMENTATION CHALLENGES

A. Data Discovery, Ownership and Legacy Records

No department can comply with notice, access, correction, breach or erasure duties without knowing what it holds, where it came from, why it is used, with whom it is shared and how long it remains. Older applications may lack data dictionaries; spreadsheets and scanned files may sit outside central inventories; and the same citizen may appear under inconsistent identifiers. A statewide inventory must be organised by processing activity and risk, not merely by application name.

B. Consent, Legitimate Use and Service Conditionality

Public bodies may be tempted to treat consent as an administrative shortcut. That is problematic when refusal means losing an essential certificate or benefit, because consent may not be meaningfully free. The better approach is to identify the statutory or policy authority for necessary processing, provide a truthful notice and seek consent only for separable optional uses. Aadhaar-linked workflows also require compliance with the Aadhaar Act and the Supreme Court's limits on mandatory authentication.20

16 Department of Information Technology & e-Governance, Government of Jharkhand, 'About', available at: https://jharkhand.gov.in/it-dept (last visited July 22, 2026).

17 Id., ch. 3, paras 3.1.1–3.1.5 and 3.2.1–3.2.3.

18 Comptroller and Auditor General of India, Report No. 1 of 2025: Information Technology Audit on Integrated Financial Management System in Jharkhand, Executive Summary, pp. 1–5.

19 The Digital Personal Data Protection Act, 2023, s. 5(3); Digital Personal Data Protection Rules, 2025, r. 3.

20 K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, (2019) 1 SCC 1; Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

C. Security, Vendors and Breach Readiness

Reasonable safeguards must cover the full delivery chain: state infrastructure, cloud or data-centre services, NIC-supported applications, software vendors, call centres and kiosks. Procurement often describes uptime and functionality more precisely than privacy. Future contracts should allocate permitted processing, confidentiality, sub-processing, location, access, logging, incident reporting, audit, return and deletion. DPDP breach duties will operate alongside the Information Technology Act, the SPDI Rules during the transition where applicable, and CERT-In's incident-reporting directions. A single state incident playbook should classify these overlapping clocks and authorities before an event occurs.21

D. Children, Welfare and High-impact Decisions

Schools, scholarships, child-protection programmes, nutrition systems and health services process children's data at scale. Verifiable parental consent can itself invite excessive collection of parental identity data. The least-intrusive verification method should be chosen, and exceptions for educational or welfare functions should not become general permission for profiling. Similarly, caste, disability, income and health information may not be separately labelled 'sensitive personal data' in the DPDP Act, but misuse can cause discrimination, stigma or exclusion. Risk controls should follow consequence, not nomenclature.

E. Privacy, Transparency and Government Exemptions

The DPDP Act amends section 8(1)(j) of the Right to Information Act, 2005, intensifying debate over personal information and public accountability. Jharkhand authorities must avoid using 'privacy' as a formula to withhold records of public expenditure, selection, licensing or official action. The public-interest override in section 8(2), severability and proactive disclosure remain central to reasoned RTI decisions. Conversely, transparency does not justify publishing complete identity documents or unnecessary beneficiary details. Publication protocols should use aggregation, masking and field-level justification.2223

The Act also contains exemptions for specified State processing and enables the Central Government to exempt notified instrumentalities in defined interests. Such provisions must be administered consistently with Puttaswamy's requirements of legality, necessity and proportionality. Exemption from a particular statutory duty should not be treated as exemption from constitutional privacy, cybersecurity or administrative fairness.24

Table 2: Jharkhand-Specific Challenges, Risks and First Controls

Challenge	Immediate Risk	Priority Control
Unknown legacy data	Inaccurate notice, uncontrolled sharing and indefinite retention	Department inventory and data-flow map
Assisted service centres	Shoulder-surfing, copied documents and operator misuse	Operator role controls, privacy screens, receipts and audit
Multiple languages and literacy levels	Nominal rather than informed notice	Layered Hindi/Santali/local-language and oral explanation

21 Information Technology Act, 2000, ss. 43A, 70B and 72A; Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011; CERT-In, Directions under s. 70B(6), Apr. 28, 2022.

22 Right to Information Act, 2005, ss. 8(2), 10 and 4.

23 The Digital Personal Data Protection Act, 2023, s. 44(3) read with the Right to Information Act, 2005, s. 8(1)(j).

24 The Digital Personal Data Protection Act, 2023, s. 17.

Challenge	Immediate Risk	Priority Control
Vendor and shared infrastructure	Responsibility gaps after breach or contract exit	Standard processor schedule, audit and deletion evidence
Children and welfare data	Profiling, exclusion and excessive identity verification	High-impact assessment and minimisation
Fragmented grievances	Citizens sent between portal, district and department	Single intake with accountable departmental resolver
RTI–privacy tension	Over-disclosure or blanket secrecy	Field-level disclosure test, masking and public-interest reasons

Figure 2: DPDP-Ready Lifecycle for Jharkhand Public Services

V. PROSPECTS AND A PRACTICAL STATE ROADMAP

The Act creates an opportunity to improve public administration beyond formal compliance. Data minimisation reduces storage and breach exposure; accurate master data reduce wrongful exclusion; clear ownership speeds correction; retention rules lower infrastructure burden; and unified grievances reveal recurring defects. Privacy is therefore compatible with reliable welfare delivery when implemented as information governance rather than as a website notice.

Jharkhand should establish a State DPDP Steering Cell within, or formally coordinated by, the Department of Information Technology and e-Governance. It should include the Law, Home, Finance, Welfare, Health, Education and Revenue departments, JAP-IT/NIC technical leadership, district representation, cybersecurity expertise and an accessibility and tribal-language perspective. The Cell would issue standards and monitor readiness; each department would remain accountable for its own purposes, records, processors and citizen responses. This allocation is preferable to a single central office purporting to become the Data Fiduciary for every system.

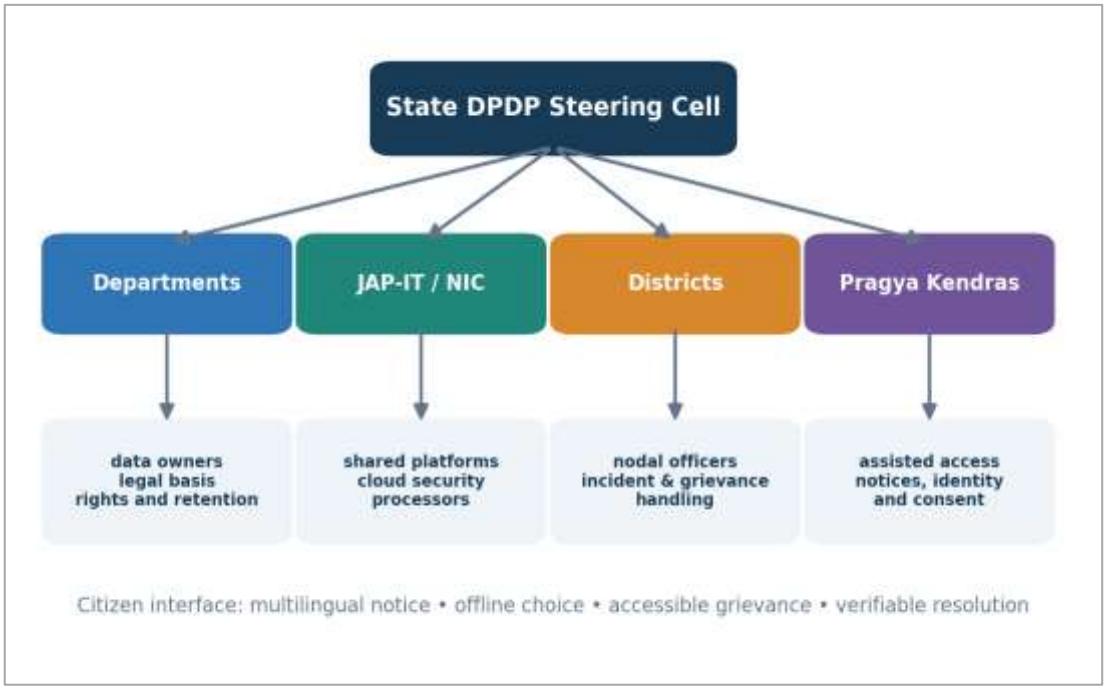

Figure 3: Proposed Governance Architecture for DPDP Implementation in Jharkhand

The first implementation product should be a common processing register covering purpose, legal basis, fields, source, recipients, system, processor, access roles, retention, security classification, rights route and owner. High-impact systems—land, health, children, policing, caste and disability benefits, recruitment and financial payments—should receive privacy and security assessments first. Although the Act formally requires impact assessment only from notified Significant Data Fiduciaries, a state may voluntarily use proportionate assessments as an administrative safeguard.

The second product should be a standard compliance kit: modular notices; a processor clause schedule; retention and legal-hold template; breach severity matrix; Data Principal request form; identity-verification standard; redaction guide; and district escalation protocol. Notices should be tested with actual users, not merely translated. A request submitted at a Pragya Kendra should generate a receipt and route to the correct department without exposing more data to the operator than necessary.

The third product should be measurable assurance. Departments should report coverage of the data inventory, privileged-access reviews, critical vendor addenda, unresolved high-risk findings, simulated breach performance, grievance age and deletion completion. Public reporting should be aggregated and privacy-preserving. Independent audit can then test evidence rather than declarations. This also responds to the documentation, business-continuity and helpdesk weaknesses identified by the CAG.

Table 3. Recommended Implementation Roadmap for Jharkhand

Period	Priority Actions	Verifiable Output
0–90 days	Constitute Steering Cell; nominate departmental owners; freeze unapproved new data fields; inventory critical systems and vendors	Government order; owner register; critical-system map
3–6 months	Map purposes and legal bases; classify high-impact processing; prepare notices, retention schedules, contracts and breach playbook	Processing register; model kit; incident exercise
6–12 months	Remediate access and logging; integrate rights intake; train districts and Pragya Kendras; review children and welfare systems	Access reviews; ticketing data; training and assessment records

Period	Priority Actions	Verifiable Output
12–18 months	Independent readiness audit; close high-risk findings; publish aggregate transparency report; test erasure and vendor exit	Audit report; closure evidence; deletion and exit certificates
Continuous	Monitor law, Board practice, cyber threats and service impact; update records after every material system change	Quarterly dashboard and annual governance review

VI. FINDINGS AND CONCLUSION

Five conclusions emerge. First, the operative legal position in July 2026 is transitional: institutional provisions are in force, while the main duties and penalties are scheduled for May 2027. Secondly, Jharkhand's most difficult task is accountability across shared platforms, departments, districts, vendors and assisted-service centres. Thirdly, legal basis must be distinguished from consent; essential public services should not depend on fictional choice. Fourthly, security and accuracy are as important as privacy notices because public databases directly affect entitlements and status. Fifthly, inclusion requires multilingual, accessible and offline-capable rights and grievance mechanisms.

The DPDP Act can become either a compliance overlay or an administrative reform. If Jharkhand begins with inventories, purpose limitation, accountable ownership, processor control, secure lifecycle management and citizen-facing remedies, the law can improve both privacy and service reliability. If implementation is postponed until the final commencement date, departments may produce hurried notices without changing underlying systems. The transition period should therefore be treated as a constitutional and managerial opportunity: to make digital government demonstrably necessary, secure, accurate and answerable to the people whose data sustain it.

SELECT BIBLIOGRAPHY

A. Constitutional, Statutory and Regulatory Materials

- The Constitution of India.
- The Digital Personal Data Protection Act, 2023.
- Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Nov. 13, 2025.
- Ministry of Electronics and Information Technology, Notification G.S.R. 843(E), Nov. 13, 2025 (phased commencement).
- Ministry of Electronics and Information Technology, Notification establishing the Data Protection Board of India, Nov. 13, 2025.
- The Information Technology Act, 2000.
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
- CERT-In, Directions relating to information security practices, procedure, prevention, response and reporting of cyber incidents, Apr. 28, 2022.
- The Right to Information Act, 2005.
- The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

B. Cases

- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
- K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, (2019) 1 SCC 1.
- People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.
- Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.
- Central Public Information Officer, Supreme Court of India v. Subhash Chandra Agarwal, (2020) 5 SCC 481.

C. Reports, Policy Materials and Institutional Sources

- Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (2018).
- Comptroller and Auditor General of India, Report No. 1 of 2025: Information Technology Audit on Integrated Financial Management System in Jharkhand.
- Government of Jharkhand, Department of Information Technology & e-Governance, official portal.
- Government of Jharkhand, JharSewa / Jharkhand e-District, official service portal.
- Ministry of Electronics and Information Technology, Digital Personal Data Protection Rules 2025—official document collection (2025).
- Press Information Bureau, Digital Personal Data Protection Rules, 2025—citizen-centric framework for responsible data use (Nov. 17, 2025).
- NIST, Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0 (2020).
- OECD, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013).

D. Selected Scholarship

- Gautam Bhatia, The Transformative Constitution (HarperCollins India, 2019).
- Rahul Matthan, Privacy 3.0: Unlocking Our Data-Driven Future (HarperCollins India, 2018).
- Daniel J. Solove, 'A Taxonomy of Privacy' 154 University of Pennsylvania Law Review 477 (2006).
- Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life (Stanford University Press, 2010).
- Woodrow Hartzog, Privacy's Blueprint: The Battle to Control the Design of New Technologies (Harvard University Press, 2018).
- Julie E. Cohen, Between Truth and Power: The Legal Constructions of Informational Capitalism (Oxford University Press, 2019).