



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

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

This is an Open Access article distributed under the terms of the Creative Commons Attribution- Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

THE BURDEN OF VERIFICATION: NAVIGATING EMPLOYEE BACKGROUND CHECKS AND DATA MINIMISATION UNDER THE DPDP FRAMEWORK

~ *Biswarup Saha*

ABSTRACT

The necessity of background verification in the corporate management has brought significant friction between itself and the strict statutory regimes regarding privacy due to the enactment of Digital Personal Data Protection (DPDP) Act, 2023 in India. On one hand, the DPDP Act allows the employee data to be processed for employment purposes, yet early erasure of the employees' background verification data due to the Act's statutory mandates exposes the employers to the liabilities of wrongful terminations and lack of evidence for the same under the Industrial Disputes Act, 1947. On the other hand, indefinite retention of the employees' background verification data risks regulatory penalties. This article analyses the legal friction between the Indian labour jurisprudence, and the DPDP Act's data minimisation principles. This article also proposes a 'Tiered Retention Framework' with the help of a comparative benchmark from the European Union's General Data Protection Regulation (GDPR) and corresponding jurisprudence. By bifurcation of the lifecycle of the employee's data, employers can implement privacy-by-design data handling processes while complying with labour law.

INTRODUCTION

With an increase in the amount of misrepresented and fraudulent credentials plaguing the resumes and CVs within the hiring pool, the corporate management in India has witnessed a monumental increase in the background verification of its employees during the hiring process. This extensive background verification plays a key role in avoiding hiring negligence.¹ Throughout the world, the practice of negligent hiring based on superficial background checks has resulted in hiring mistakes, costing companies significant financial and goodwill damages. Due to the prevalent manual method of screening for the background verification process being outdated, the corporate management leaves loopholes in the security of hiring the right people, thereby increasing the hiring risk.² Thus, the corporate management has become exhaustive in its approach of background verification, including but not limited to criminal history, previous employment verification, financial verification, etc., which has become the standard practice of corporate risk management.

However, the implementation of the Digital Personal Data Protection (DPDP) Act, 2023, published by the Ministry of Electronics and Information Technology (MeitY) has introduced statutory changes for the privacy framework in India, and which has created friction points for handling data: retention policies for data have become conflict points with respect to employees' data privacy, and erasure mandates have become disputable due to the labour practices.³ While the DPDP Act allows the retention of employee data for employment purposes, this indefinite retention period creates a paradox of verification due to statutory mandates, which can be resolved with a 'Tiered Retention Framework'.

SCOPE OF "EMPLOYMENT PURPOSES"

Within the employment context, Section 7(i) of the DPDP Act permits a Data Fiduciary (here, the employer) to process the personal data of a Data Principal (here, the employee) without the requirement of their explicit and affirmative consent, provided the processing of this data is strictly for the purposes of employment or those related to safeguarding the employer from loss or liability, such as the prevention of corporate espionage.⁴

¹ European Commission, *Pre-employment Screening*, https://ec.europa.eu/employment_social/empl_portal/transnational_agreements/Gepe_pre-employmentscreening_EN.pdf

² Deloitte India, *DashVerify: Employee Background Verification Services*, <https://www.deloitte.com/in/en/services/consulting/services/risk-regulatory-forensic/dashverify.html>

³ Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).

⁴ NovoJuris, *Navigating the Legitimate Use Exemption for Employee Data Under the DPDP Act, 2023*, <https://www.novojuris.com/thought-leadership/navigating-the-legitimate-use-exemption-for-employee-data-under-the-digital-personal-data-protection-act-2023.html>

Upon analysis of Section 7(i), it is found that only by maintaining transparency, necessity and limitation of usage shall the data be handled without triggering workplace surveillance or data hoarding through human resource operations and practices. Although Section 7 allows bypassing of consent, the employers must ensure that the existence of a current employer-employee relationship is present to enact this bypass through provisions. And as soon as the employee is no longer employed with their employer, the criterion of safeguarding the employer's interest becomes irrelevant. This creates an ambiguity regarding the statutory exemption to not only the prospective candidates during the pre-hire screening phase, but also the non-permanent staff and contractual hires. Therefore, employers generally prefer applicability of consent under Section 6 of the DPDP Act for background verification, and the invocation of Section 7(i) is applied only after the employment is formally executed.⁵

According to Rule 3 of Digital Personal Data Protection Rules, 2025, where consent is required, such as in pre-employment screening, such consent notice must be clearly communicated by the employer with the employees, and also provide a list of their personal data being processed along with specific purposes.⁶

Under the DPDP Act, the engagement of third-party verification vendors acting as Data Processors conducting verification process fundamentally alters the liability structure for the employers, because the Act requires the Data Fiduciary to bear complete and non-delegable regulatory responsibility for any compliance failures or data breaches from the Data Processors.⁷ This system requires execution of Data Processing Agreements that strictly define data processing instructions, create security safeguards, and enforce breach notification timelines. To resolve vulnerabilities arising from these third-parties, established industry bodies recommend the utilisation of decentralised blockchain verification platforms, which use automated system to store data cryptographically. This cryptography ensures tamper-proof sensitive personal data being safeguarded from unauthorised access, thereby significantly reducing reliance on vulnerable third-party verification vendors.⁸

Three strategic shifts are required to transition from the pre-existing verification procedures to the ones compliant with the DPDP Act, 2023. First, data minimisation by limiting financial and criminal history checks to role-specific relevancy instead of collecting familial, financial, and residential data for all roles. Second, the processor liability must shift entirely to the

⁵ *Id.*

⁶ Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Rule 3 (India).

⁷ Digital Personal Data Protection Act, No. 22 of 2023, § 8(2), India Code (2023).

⁸ NASSCOM Community, *Unlocking Efficiency and Transparency: Role of Blockchain in Background Verification*, <https://community.nasscom.in/communities/blockchain/unlocking-efficiency-and-transparency-role-blockchain-background>

employer, giving them responsibility to necessitate agreements with audit rights.⁹ Third, the transparency brought about by Rule 3 of the DPDP Rules, 2025, necessitates employers to opt for listed data being collected from the employees with standalone, clearly communicated privacy policies and practices.¹⁰

ERASURE DILEMMA VERSUS LABOUR LIABILITIES

The most important point of friction between the statutory provisions of data handling by the DPDP framework and the Indian corporate management is the management of the lifecycle of such data. Section 8(7) of the DPDP Act strictly requires a Data Fiduciary to erase personal data as soon as it is reasonable to assume that the specified purpose for which such data was being used is no longer being served, or upon the withdrawal of consent by the employee, unless the retention of such data is expressly required by another applicable law being in force.¹¹

The purpose of a pre-hire background verification is to ascertain the suitability, integrity, and validity of credentials of a potential candidate before confirming their employment, and once the employment's probation period ends, the purpose of the data collected from such employees concludes. Furthermore, upon the termination of the employment of the employee, Section 7(i) is valid to be invoked, and the data collected from them is subject to the erasure or anonymisation upon the employee's request.¹² The Data Protection Board of India, which is established under the DPDP Act to enforce these provisions, possesses the authority to penalise non-compliance to these provisions.¹³ Therefore, employers are required to implement a personal data retention policy that defines for how long the data of the employees is kept after they leave.¹⁴

However, the data erasure provision collides with the Indian labour jurisprudence and its requirement of evidence by the industrial tribunals and labour courts to consider such evidence leading to the proportionality of termination orders. Therefore, the employer is required to keep primary documented evidence for such compliance with the requirements.¹⁵

The Supreme Court of India has consistently held that any employment obtained through deceit, forged documents, or deliberate suppression of material facts vitiates the employment contract. In the landmark jurisprudence governing the suppression of criminal antecedents, the

⁹ Digital Personal Data Protection Act, No. 22 of 2023, § 8(2), India Code (2023).

¹⁰ Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Rule 3 (India).

¹¹ Digital Personal Data Protection Act, No. 22 of 2023, § 8(7), India Code (2023).

¹² NovoJuris, *supra* note 4.

¹³ Establishment of the Data Protection Board of India, G.S.R. 844(E) (Nov. 13, 2025).

¹⁴ NovoJuris, *supra* note 4.

¹⁵ Industrial Disputes Act, No. 14 of 1947, § 11A, India Code (1947).

Supreme Court has affirmed the employer's absolute discretion to terminate the employment if deliberately withheld material information was important to the role and compromised the trust of the employment relationship.¹⁶ Similarly, false declarations in attestation forms amount to moral turpitude, and subsequent acquittals do not result in reversing the effect of initial fraud.¹⁷

If an employer faithfully complies with Section 8(7) of the DPDP Act by permanently deleting the background verification data immediately after the employee's confirmation of employment, then they destroy the foundational evidence of the employee's initial declarations. If it is discovered some time later that the employee fabricated their prior corporate experience or concealed a material criminal conviction, the employer will lack the evidentiary basis to defend a termination order before an Industrial Tribunal.¹⁸ The DPDP Act provides an exemption for retention necessary for compliance with any law being in force, yet whether the defence of a labour dispute satisfies the data handling standard remains debatable.

EXTRATERRITORIAL BENCHMARK OF GDPR

The friction existing between retaining employment data and exercising privacy rights is not an exclusively Indian phenomenon, but a point of debate within the global data governance. And a comparative analysis with the European Union's General Data Protection Regulation (GDPR) offers valuable insights into resolving this debate. Article 88 of the GDPR specifically addresses data processing with regard to employment, formally permitting Member States to enact specific rules which are targeted to ensure the protection of human dignity, legitimate interests, and the fundamental rights of employees regarding workplace data processing.¹⁹

The European Data Protection Board (EDPB) establishes a rigorous proportionality test for background verification, acknowledging the objective of protecting business assets. Therefore, employers must not rely on sweeping, indiscriminate background verifications for all the staff members, but rather, intricately collect data specified to roles and their related operational risks.²⁰ European regulators and data protection authorities operationalise these privacy principles and practices aggressively. In a notable enforcement action by the UK Information Commissioner's Office (ICO), a major service provider known as Capita was fined £8,000,000

¹⁶ Avtar Singh v. Union of India, (2016) 8 S.C.C. 471 (India).

¹⁷ Kendriya Vidyalaya Sangathan v. Ram Ratan Yadav, (2003) 3 S.C.C. 437 (India).

¹⁸ Industrial Disputes Act, No. 14 of 1947, § 11A, India Code (1947).

¹⁹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 88, 2016 O.J. (L 119) 1.

²⁰ Article 29 Data Protection Working Party, *Opinion 2/2017 on Data Processing at Work*, WP 249 (June 8, 2017).

for failing to ensure appropriate security measures during the processing of personal data, which included employment and pension information of the employees. The regulatory body emphasised that failing to protect sensitive data, and retaining it without security measures to prevent unauthorised access, constitutes a severe violation of core data processing principles and practices.²¹ Thus, European employers can retain only the necessary data points of an employee after their employment is confirmed to identify and assess their suitability of the qualifications for the required role. All other irrelevant information obtained from the background check are deleted as per the employer's compliance with the regulatory bodies. This benchmark drawn from the European Union indicates the weakness of the defence in retaining background verification data under any circumstance of necessity arising from the employers that may breach privacy safeguards and labour disputes in the future.

CONCLUSION

The statutory friction between the DPDP Act's data erasure provisions and the necessitated evidentiary requirements of Indian labour law practices places the corporate management in a precarious legal position. Blanket policies for data retention from background verifications exposes the Data Fiduciaries to regulatory penalties for violating Section 8(7) of the DPDP Act, 2023, and failing to maintain security safeguards for the data.²² Conversely, the premature deletion of this data exposes the management to be accused of wrongful terminations, exorbitant litigation costs, and an inability to enforce contractual integrity when fraud by the employee is ultimately discovered.

To resolve this problem, corporate management should consider implementing a 'Tiered Retention Framework', which reconciles data minimisation with labour law compliance through a bifurcated approach to the data lifecycle.

The first tier involves the permanent retention of an abstracted compliance certificate. Upon the successful completion of a background verification, the Data Processor (here, the background verification vendor) should generate a generic 'Pass/Fail' compliance certificate. With the help of tools like automated parsing and blockchain-based decentralised storage, Data Processors can process verification outcomes and ensure tamper-proof data integrity without storing the employee's data indefinitely.²³ This certificate must actively remove all sensitive personal data and retain only high-level metadata. Because this abstracted certificate forms the

²¹ GDPRhub, *ICO (UK) - Capita plc and Capita Pension Solutions Ltd*, [https://gdprhub.eu/index.php?title=ICO_\(UK\)_-_Capita_plc_and_Capita_Pension_Solutions_Ltd&mtc=today](https://gdprhub.eu/index.php?title=ICO_(UK)_-_Capita_plc_and_Capita_Pension_Solutions_Ltd&mtc=today)

²² Digital Personal Data Protection Act, No. 22 of 2023, § 8(7), India Code (2023).

²³ Deloitte India, *supra* note 2; NASSCOM Community, *supra* note 8.

foundational basis of the ongoing employment contract and serves as the primary evidentiary document, it falls squarely under the "employment purposes" exemption of Section 7(i) of the DPDP Act, allowing it to be retained permanently in the employee's human resources file without causing issues regarding data privacy.²⁴

The second tier requires the third-party verification vendors to destroy all sensitive data used to generate the compliance certificate. Through stringent Data Processing Agreements formulated under the DPDP Act between the employers and the third-party verification vendors, employers must legally mandate that the vendor permanently destroys the background verification data within a fixed period soon after onboarding.²⁵

By adopting this tiered framework, the Data Fiduciaries can satisfy the data erasure requirements of Section 8(7) of the DPDP Act by purging unnecessary sensitive data once the initial hiring process is concluded.²⁶ Subsequently, by retaining the employee's original signed declarations alongside a cryptographically verifiable compliance certificate, the employer preserves the documentary evidence required to satisfy judicial scrutiny should the employee's representations of qualifications later get exposed as fraudulent.²⁷ This framework offers a sustainable, legally defensible path forward in India's rapidly evolving data regulation landscape.

²⁴ Digital Personal Data Protection Act, No. 22 of 2023, § 7(i), India Code (2023).

²⁵ *Id.* § 8(2).

²⁶ Establishment of the Data Protection Board of India, G.S.R. 844(E) (Nov. 13, 2025).

²⁷ Industrial Disputes Act, No. 14 of 1947, § 11A, India Code (1947).