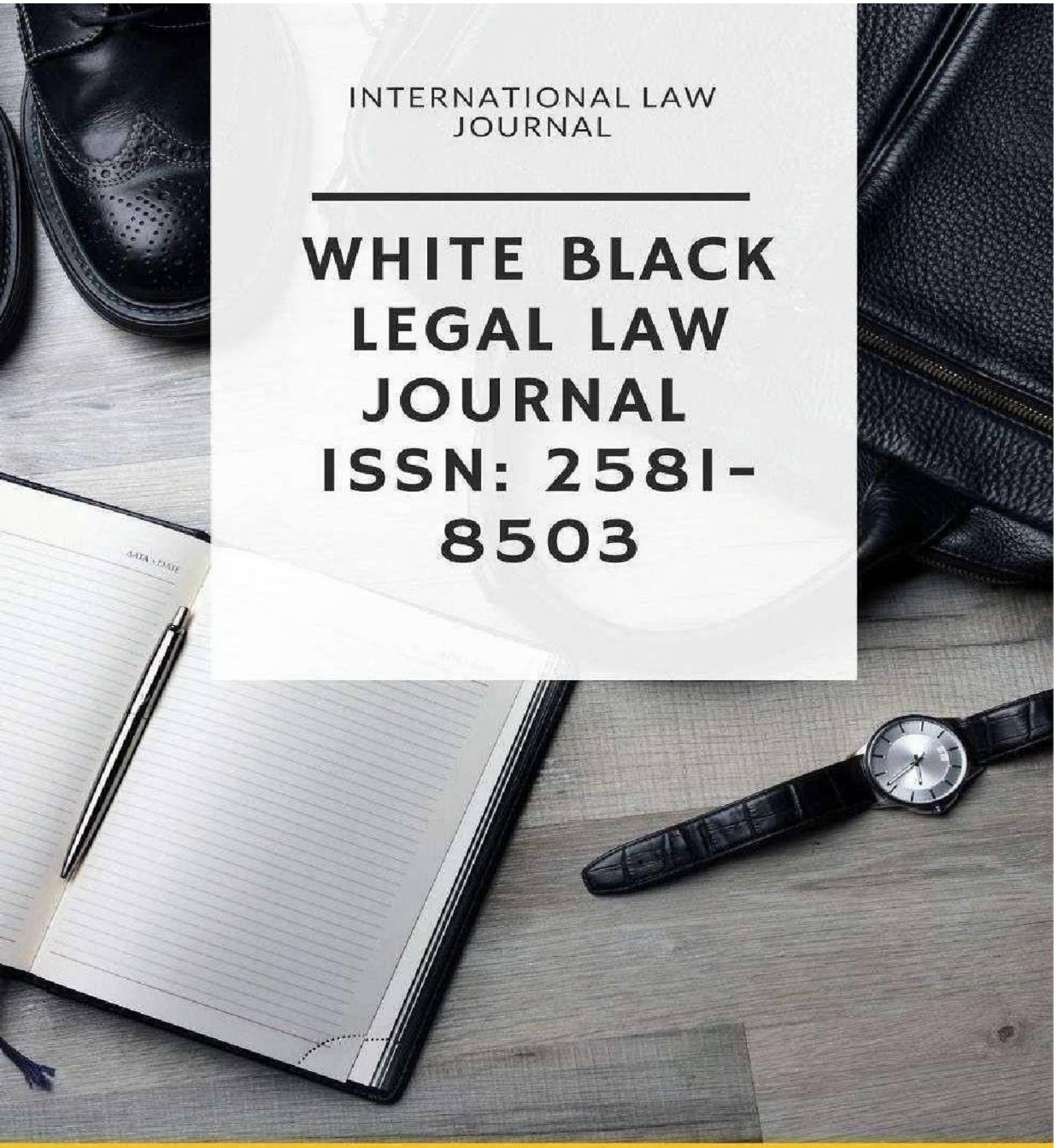

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

www.whiteblacklegal.co.in
Volume 3 Issue 8 | June 2026 ISSN: 2581-8503

FROM CONTRACTS TO COMPLIANCE: PRACTICAL INSIGHTS INTO DATA PROTECTION, EMPLOYMENT OBLIGATIONS, AND CORPORATE RISK MANAGEMENT

AUTHORED BY – PRERNA MAHESHWARI
MDU, Rohtak

I. ABSTRACT

Corporate risk is no longer contained within a single legal department or a single document. A vendor agreement, an offer letter, a workforce-monitoring tool, and a board disclosure can all concern the same factual event: the collection, use, retention, or disclosure of personal data. This article examines the practical convergence of contract management, the Digital Personal Data Protection Act, 2023, the Digital Personal Data Protection Rules, 2025, India's newly implemented Labour Codes, the POSH regime, and listed-company risk governance. It argues that contractual drafting is necessary but insufficient. A company is able to demonstrate compliance only when the contractual promise is translated into an identifiable process, responsible owner, evidentiary record, escalation route, and board-level review.

The article develops a contract-to-control model for Indian enterprises. It shows why broad employee consent should not become a shortcut for intrusive data practices; why labels such as consultant or contractor cannot override the actual character of a work relationship; and why a board should receive evidence of control performance rather than a catalogue of policies. It also proposes a phased implementation programme for organisations preparing for the substantive DPDP framework, which is scheduled to come into force in May 2027. The article's principal claim is that effective compliance is not a collection of clauses. It is the capability to prove, at short notice, how a legal commitment works in practice.

Keywords: *Data Protection, Digital Personal Data Protection Act, Employment Law, Labour Codes, Corporate Governance, Risk Management, POSH, Vendor Management, Workplace Surveillance.*

II. INTRODUCTION

The contemporary Indian enterprise operates through a dense network of contractual and technological relationships. Recruitment may be conducted through a cloud-based platform. Payroll may be administered by an external processor. Attendance may be recorded by a biometric device. Employee communications may be stored by a collaboration provider. A listed company may need to disclose a cyber incident while simultaneously preserving an internal investigation. None of these events belongs neatly to one legal category. Each can involve private-law allocation of risk, statutory labour obligations, privacy duties, information-security controls, evidentiary questions, and corporate-governance accountability.

This convergence changes the significance of contract drafting. Traditionally, the contract was treated as the principal mechanism for allocating rights and liabilities between parties. In a regulated organisation, it is also an operational representation: it says what data may be processed, what a supplier may do, when an employee may access a system, how an incident will be reported, and what happens when the relationship ends. A clause that cannot be performed is not a control. At best, it records an aspiration; at worst, it supplies evidence that the organisation promised a safeguard it never built.

India's legal landscape gives this question unusual urgency. The Central Government announced implementation of the Code on Wages, 2019, the Industrial Relations Code, 2020, the Code on Social Security, 2020, and the Occupational Safety, Health and Working Conditions Code, 2020 with effect from 21 November 2025. The reforms seek to consolidate twenty-nine central labour laws and give statutory force to appointment letters, wider social-security coverage, and protection for modern forms of work.1 In parallel, the DPDP Act and the DPDP Rules are being brought into force in stages. Most provisions concerning notice, consent, legitimate uses, data-fiduciary obligations, data-principal rights, breach management, and penalties are scheduled to commence eighteen months after the notification of 13 November 2025—namely, in May 2027.2

The transition should not be misunderstood as a period in which businesses may postpone compliance design. Existing obligations under the Information Technology Act, 2000, the SPDI Rules, sectoral requirements, contractual confidentiality duties, labour law, and constitutional values continue to matter. More importantly, the transition period is the only sensible time to build data maps, vendor governance, workforce classifications, and incident-

response capability before their absence becomes a regulatory event.

III. THE CONTRACT-TO-CONTROL PROBLEM

1. Why clauses do not complete compliance

An agreement can allocate commercial loss between the parties. It cannot, by itself, eliminate a regulator's concern, reverse the disclosure of personal information, restore a worker's dignity after unlawful monitoring, or prevent a listed entity from having to explain a material incident to investors. This distinction is central. Indemnities, limitation-of-liability clauses, and warranties remain important; however, they operate after failure. Compliance design is concerned with preventing failure and preserving the ability to respond credibly when it occurs. The practical question for every material clause is therefore evidentiary: what could the organisation produce tomorrow to show performance? If a processor contract requires reasonable security safeguards, the company should be able to identify the processor's security assessment, audit rights, incident contacts, subcontractors, and remediation status. If an employment contract requires protection of confidential information, the company should be able to show access controls, training, classification of information, and a documented offboarding process. If a vendor must erase data at termination, the company should hold an accountable record of return, deletion, or lawful retention.

A useful compliance inventory should convert each material commitment into a control entry containing the following fields: the purpose of the processing or activity; the data or asset involved; the business owner; the system and relevant vendor; the legal basis or statutory obligation; the required safeguard; the evidence produced by the safeguard; the escalation trigger; and the date of the next review. This inventory allows legal, HR, procurement, information security, and risk functions to discuss the same risk in a common language.

2. The lifecycle of a contractual promise

The contract lifecycle should be connected to the data lifecycle. At onboarding, procurement should classify the vendor's access and require due diligence proportionate to the risk. During performance, the contract owner should monitor material changes such as a new subcontractor, new location of processing, or expanded purpose. At exit, the organisation should check return of assets, revocation of access, deletion or retention of data, transition of records, and survival of confidentiality and assistance obligations. This is particularly important where the supplier has access to employee, customer, financial, or investigation data.

Such an approach also prevents a common drafting error: treating a long privacy schedule as a substitute for a clear scope of processing. The most useful provisions identify the subject matter, purpose, categories of data, affected persons, duration, instructions, permitted recipients, security expectations, breach-notification timetable, audit mechanics, and deletion/return procedure. The agreement must also allocate the consequences of a request from a data principal or a regulator. A processor cannot meaningfully assist with a request if the controller has not identified where the relevant data sits.

IV. DATA PROTECTION AND THE EMPLOYMENT RELATIONSHIP

1. Consent, legitimate uses, and the imbalance of employment

The DPDP Act describes consent as free, specific, informed, unconditional, and unambiguous.3 That formulation has special significance in the workplace. An employee asked to accept a sweeping privacy clause in an offer letter, or to enrol in a monitoring system as a condition of continued employment, may possess no realistic ability to negotiate. Employers should therefore avoid treating a broad contractual acceptance as an all-purpose permission for future collection, analytics, surveillance, or sharing.

The Act recognises a legitimate-use basis for processing personal data for purposes of employment or to safeguard the employer from loss or liability.4 This should be understood as a functional and limited basis, not as a blanket licence. Payroll, statutory benefits, tax deductions, access management, fraud prevention, health and safety, internal investigations, and preservation of trade secrets may justify carefully bounded processing. But each use should be connected to a defined objective and should collect no more than the organisation can explain as necessary.

A sound workplace privacy programme distinguishes at least six data contexts: recruitment; workforce administration; benefits and statutory compliance; performance management; investigations; and security or monitoring. They have different purposes, access needs, sensitivities, retention periods, and consequences for the person affected. A single privacy notice cannot responsibly perform the work of six separate notices and six separate accountability assessments.

2. Monitoring requires a necessity discipline

Remote work and digital collaboration have expanded the means available to employers. GPS tracking, keystroke logging, screenshots, webcam activation, biometric attendance, communications review, and AI-generated productivity scores can now be deployed cheaply

and continuously. That technical availability does not establish legal necessity. The appropriate question is whether a less intrusive measure can reasonably achieve the same objective.

Before deployment of a high-impact monitoring practice, an organisation should produce a short written assessment: the legitimate business objective; the affected population; the data fields collected; why less intrusive alternatives are insufficient; the accuracy and bias risks; the human decision-maker; access restrictions; the retention period; an employee notice; and the complaint or challenge route. The assessment should be reviewed when the tool changes materially. This is not an imported GDPR ritual. It is a practical way to demonstrate fairness, accountability, and proportionality in an employment setting.

Recent legal scholarship has persuasively drawn attention to the workplace-surveillance gap in India and to the constitutional importance of legality, legitimate purpose, and proportionality after K.S. Puttaswamy (Retd.) v. Union of India.5 The corporate lesson is pragmatic: a business should secure its systems through encryption, access controls, task-based performance review, and targeted incident controls before resorting to continuous observation of individual workers.

3. Retention, access, and exit

Employee data is often kept by default rather than by decision. Former employees may remain in talent databases, collaboration accounts, benefits portals, access-control logs, and vendor systems long after a practical purpose has ended. The DPDP framework's purpose limitation and erasure expectations make this approach increasingly difficult to defend. Data should be retained because a documented business or legal purpose remains, not because deletion is inconvenient.

Access must be similarly deliberate. HR personnel, line managers, payroll administrators, security staff, investigators, and external advisers may each need limited information for different reasons. Role-based permissions, access logs, and periodic review create a defensible boundary between proper administration and curiosity. At exit, a coordinated process should revoke system access, retrieve devices, preserve litigation holds where appropriate, separate personal from business information, and send deletion instructions to relevant vendors.

V. EMPLOYMENT OBLIGATIONS BEYOND THE LABEL

1. Classification follows substance

Businesses frequently use the language of consultancy, retainership, agency, or independent contracting. Such language can be commercially useful, but it cannot conclusively determine whether the worker is, in substance, an employee. Indian adjudication has repeatedly examined

the degree of control, integration into the enterprise, economic dependence, remuneration structure, power of dismissal, and whether the individual carries a business risk of their own.6 This matters beyond tax treatment. A misclassification may affect wages, social security, gratuity, working conditions, occupational safety, principal-employer exposure, and workplace-protection duties. It may also undermine data-governance positions. A company that dictates a worker's schedule, equipment, location, performance metrics, and access credentials creates a factual record of organisational integration, whatever the contract calls the relationship.

The most defensible workforce programme begins with a classification register. It records each category of worker, the relevant entity, location, manager, engagement document, payment channel, statutory benefits, and the principal facts supporting the classification. The register should be reviewed whenever an individual's engagement becomes long-term, exclusive, closely supervised, or embedded in core business operations. The objective is not to eliminate flexible work. It is to ensure that flexibility is not purchased through inaccurate legal characterisation.

2. Appointment letters, conditions of work, and change management

The Labour Codes' formalisation agenda makes written and accurate employment documentation increasingly significant. The Ministry of Labour and Employment has specifically described appointment letters as mandatory for workers and has emphasised benefits for fixed-term employees, including equal treatment with permanent employees and gratuity eligibility after one year of continuous service.7 Contracts should therefore identify designation, wages, benefits, location or remote-work arrangement, reporting, hours, confidentiality, intellectual property, grievance routes, applicable policies, and lawful conditions for variation.

Change management should not be concealed in boilerplate. An employer may need to alter reporting lines, workplace arrangements, systems, or benefits structures; but a clause permitting unilateral change should not become an assumption that consultation is unnecessary. NLU scholarship has highlighted the unequal bargaining position in standard-form employment contracts and the weaknesses of treating notice alone as a complete answer to consent and fairness.8 A careful employer records the business rationale, the class of employees affected, the legal conditions, consultation steps, and effective date of any material change.

VI. POSH, INVESTIGATIONS, AND CONFIDENTIAL INFORMATION

Workplace investigations generate some of the most sensitive information held by an enterprise. A complaint may include personal narrative, medical information, witness accounts, CCTV material, chat records, location data, and allegations about identified individuals. Mishandling such records creates a second injury: it can compromise the fairness of the inquiry while exposing the company to confidentiality, privacy, retaliation, and reputational risk.

The POSH Act requires an employer to constitute an Internal Committee in the prescribed circumstances and specifies its composition, including a senior woman employee as Presiding Officer and an external member familiar with the relevant issues.9 The committee should be operational, not nominal. It requires training, a secure reporting channel, independence, defined conflict procedures, timely inquiry, reasoned records, confidentiality safeguards, and a mechanism to identify retaliation.

Investigations should apply a need-to-know rule. The inquiry team should collect only information relevant to the allegation, preserve the chain of custody for electronic evidence, restrict access to the case file, record external disclosures to counsel or specialists, and make a documented retention decision after closure. Communications monitoring should not be expanded merely because an investigation has begun. The scope should reflect the allegation and be periodically tested against necessity.

VII. CORPORATE RISK MANAGEMENT AND BOARD OVERSIGHT

1. From policy reporting to control reporting

A board cannot administer every compliance process. It can, however, insist that management reports the performance of controls rather than merely the existence of policies. A statement that the company has a privacy policy says little about whether the company knows its processors, tests its incident plan, deletes data, or resolves high-risk access exceptions. Effective risk reporting connects the issue to an owner, measure, threshold, remediation plan, and escalation route.

For listed entities, this is reinforced by SEBI's corporate-governance architecture. Regulation 4 of the LODR Regulations embeds risk management, financial and operational control, and compliance in the principles governing obligations; Regulation 27 requires reporting on corporate governance, including cyber-security incidents, breaches, or loss of data or

documents as specified by the Board.10 BRSR Core has also made workforce and value-chain information increasingly assurance-sensitive.11

The board or Risk Management Committee should receive a small number of decision-useful metrics: high-risk vendors without current assessments; systems processing sensitive employee or customer data without an owner; completion of access reviews; unresolved security findings; time taken to detect and contain simulated incidents; workforce-classification exceptions; delayed investigations; and repeated policy violations. A narrative should explain material movement, not obscure it.

2. Third-party risk as enterprise risk

Outsourcing does not outsource accountability. A payroll provider, recruiter, cloud host, background-verification firm, and AI vendor can each create exposure for the company that selected and instructed them. Vendor due diligence should be risk-tiered: basic for low-risk suppliers; deeper review for those processing personal data, accessing production systems, interacting with workers, making recommendations about individuals, or supporting regulated activities.

The vendor file should hold the due-diligence result, contract, data-flow summary, named business owner, security/contact details, audit evidence, material subcontractors, and remediation record. High-risk contracts should be reviewed at renewal and after a material incident. This approach allows a company to answer the regulator's practical question: not simply whether a clause existed, but what the company did to know and manage the risk.

VIII. A PRACTICAL IMPLEMENTATION ROADMAP

A realistic programme begins with high-impact processes rather than a wholesale policy rewrite. In the first thirty days, the organisation should establish a joint legal-HR-security-procurement working group and identify its ten most consequential data-and-workforce pathways: recruitment, onboarding, payroll, attendance, benefits, performance management, investigations, remote work, vendor access, and offboarding. For each pathway, it should identify the data, purpose, system, owner, vendor, retention period, legal basis, contractual control, and evidence available.

In the next thirty days, the organisation should remediate priority gaps: untracked data sharing,

missing vendor agreements, obsolete access, overbroad monitoring, absent notices, unresolved worker classifications, incomplete appointment documentation, and untested incident-response procedures. It should also establish escalation thresholds for suspected breaches, POSH complaints, employment-status disputes, and significant vendor failures.

In the final thirty days, the organisation should test rather than merely document. A breach tabletop can test whether legal, security, HR, communications, and management know their roles. A sample vendor audit can test whether contractual rights yield usable evidence. An employee-data access review can test whether permissions reflect real roles. A board report can test whether risk information is concise enough to drive action. The resulting records become the first version of the organisation's compliance evidence base.

IX. CONCLUSION

The movement from contracts to compliance does not diminish the value of legal drafting. It restores the contract to its proper role: a clear statement of obligations that can be operationalised, monitored, and proved. The most serious failures occur when an agreement promises safeguards that systems, people, and governance arrangements cannot deliver.

India's phased data-protection regime and implemented Labour Codes create a rare opportunity for enterprises to connect legal obligations before enforcement pressure makes the connection unavoidable. The correct question is not, 'Do we have the clause?' It is, 'Can we show how the promise works, who owns it, what evidence proves it, and how failure reaches the board?' A company that can answer those questions is not merely better prepared for compliance; it is better prepared to act fairly toward workers, customers, investors, and business partners.

X. REFERENCES

1. Ministry of Labour & Employment, Government Announces Implementation of Four Labour Codes to Simplify and Streamline Labour Laws (21 Nov. 2025).
2. Ministry of Electronics and Information Technology, Notification G.S.R. 843(E), Digital Personal Data Protection Act, 2023—Commencement Notification (13 Nov. 2025).
3. Digital Personal Data Protection Act, 2023, s. 6.
4. Digital Personal Data Protection Act, 2023, s. 7(i).

5. Pragya Mittal, Surveillance at Work: Advocating the Right to Not be Monitored, Law School Policy Review (12 Aug. 2025); K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
6. Dharangadhra Chemical Works Ltd. v. State of Saurashtra, AIR 1957 SC 264; Ram Singh v. Union Territory, Chandigarh, (2004) 1 SCC 126.
7. Ministry of Labour & Employment, supra note 1.
8. Aaditi Sinha, The Myth of (Fragile) Consent: Unilateral Changes and Indian Employment Law, Law School Policy Review (30 Dec. 2024).
9. Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013, s. 4.
10. Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015, regs. 4, 27 (as amended up to 22 Jan. 2026).
11. SEBI/HO/CFD/CFD-SEC-2/P/CIR/2023/122, BRSR Core—Framework for Assurance and ESG Disclosures for Value Chain (12 July 2023).
12. Siddharth Johar, Surveillance Backdoors and the Data Protection Regime in India, NLSIR Online (22 May 2026).
13. Gargi Srivastava & Dhruv Singhal, The Exigency of a Journalistic Exemption in India's Data Protection Framework, 18 NUJS L. Rev. 1 (2025).
14. Sarrah Darugar & Mustafa Rajkotwala, Publicly Available Data under the DPDP Act: The Limits of Exemptions in AI-Driven Processing, Law School Policy Review (13 Jan. 2026).