CROSS-BORDER OUTSOURCING OF EMPLOYEE DATA BY TRANSNATIONAL CORPORATIONS: AN ANALYSIS OF DATA PRIVACY, INFORMATION SECURITY AND REGULATORY CHALLENGES IN INDIA

Naman Kishore, CB&IL LLM, Amity Law School, Amity University, Noida[1]

ABSTRACT

The globalisation of business has made cross-border employee data transfers essential to transnational corporate operations. Multinational enterprises increasingly outsource payroll, recruitment, human resource management, employee monitoring and data storage to overseas service providers. Although these arrangements enhance operational efficiency, they raise significant concerns regarding privacy, confidentiality, cybersecurity, accountability and employee rights. Employee data often includes sensitive personal, financial, health, biometric and professional information, making its protection particularly important. This paper examines the legal and regulatory framework governing cross-border outsourcing of employee data by transnational corporations in India. It analyses the constitutional right to privacy, the Digital Personal Data Protection Act, 2023, the Information Technology Act, 2000, relevant rules, cybersecurity obligations and contractual safeguards, alongside international approaches to data transfers. The paper highlights challenges concerning employee consent, cross-border transfers, data security, processor accountability, workplace surveillance and regulatory enforcement. It argues that despite India's evolving data protection framework, significant implementation and accountability gaps remain. It recommends a risk-based regulatory approach emphasising transparency, meaningful employee protection, enforceable contractual obligations, cybersecurity standards and effective regulatory supervision.

Keywords: Employee data; cross-border data transfers; transnational corporations; data privacy; information security; Digital Personal Data Protection Act, 2023; India; outsourcing; data fiduciary; data processor.

[1] CB&IL LLM, Amity Law School, Amity University, Noida

1. INTRODUCTION

1.1 Background and context

The contemporary corporate enterprise is increasingly organised across national borders. A transnational corporation may recruit employees in India, maintain its global human-resources database in another jurisdiction, outsource payroll to a service provider in a third country, use cloud infrastructure distributed across several regions, and rely on a central analytics platform to assess workforce performance. These arrangements are enabled by digital platforms, cloud computing, remote access technologies, enterprise resource planning systems and specialised business-process outsourcing providers. Employee information can therefore move across borders continuously, often without the employee knowing where each category of information is stored, accessed, analysed or retained.[2] The cross-border outsourcing of employee data is not confined to administrative information. Human-resource systems may process names, addresses, contact details, bank-account information, tax identifiers, salary records, attendance, leave history, medical certificates, insurance details, biometric data, background-check reports, disciplinary records, performance evaluations, workplace communications and location data. Some information is collected directly from employees, while other information is generated through workplace systems, monitoring tools, access-control devices, recruitment platforms and productivity software. The combination of these datasets can reveal intimate aspects of an employee's life, health, behaviour, financial position and professional prospects.[3]

Outsourcing offers genuine commercial advantages. A corporation may centralise payroll processing to reduce duplication, obtain specialist cybersecurity services, use global human-resource platforms, improve continuity, standardise compliance and achieve economies of scale. However, outsourcing also separates the organisation making decisions about employee data from the entity that physically processes or hosts it. This separation complicates the identification of responsibility when information is accessed without authority, transferred onward, retained longer than necessary, exposed through a cyberattack or used for a purpose unrelated to the original employment function.[4]

The legal problem is consequently multidimensional. Data protection law asks whether personal data is processed lawfully, fairly and transparently. Information-security law asks whether reasonable safeguards are implemented to prevent unauthorised access, alteration, disclosure or destruction. Employment law raises questions about consent, power imbalance, surveillance and dignity. Contract law determines the obligations of the employer, service provider and sub-processors. International law

[2] International Labour Organization [ILO], 1997; European Parliament & Council of the European Union, 2016, Recitals 5–6
[3] ILO, 1997; Ministry of Communications and Information Technology, 2011, Rules 2–5
[4] European Parliament & Council of the European Union, 2016, Arts. 28 and 32; ILO, 1997

and regulatory policy address the jurisdiction of the State where the employee works, the destination country, and the location of infrastructure or corporate decision-making. A workable framework must coordinate these overlapping areas rather than treating cross-border outsourcing as a purely technical or contractual issue.[5]

1.2 Statement of the research problem

India's digital economy and services sector are deeply connected with global business operations. Indian employees may work for Indian subsidiaries of foreign corporations, Indian outsourcing firms processing information for overseas clients, or domestic enterprises using foreign cloud and HR vendors. The same data may pass through multiple entities and jurisdictions. Yet, employees may not be able to identify the complete processing chain, understand the destination-country safeguards, challenge excessive monitoring, or obtain timely remedies after a breach. The employer may rely on standard vendor contracts, privacy notices or employee consent forms, although these instruments may not adequately address the practical risks of international processing.

The central research problem is whether India's evolving data-protection framework provides sufficient and coherent protection for employee data when it is outsourced and processed across borders by transnational corporations. The issue is not merely whether a transfer is technically permitted. It is whether the legal framework ensures transparency, purpose limitation, data minimisation, security, accountability, effective employee rights and accessible remedies throughout the data lifecycle, including onward transfers and deletion.

1.3 Research questions

1. What are the principal business models and legal risks associated with cross-border outsourcing of employee data by transnational corporations?

2. What constitutional, statutory and regulatory protections govern the collection, processing, storage and transfer of employee data in India?

3. How does the Digital Personal Data Protection Act, 2023 regulate data fiduciaries, data processors and cross-border transfers in employment-related processing?

4. Are consent, notice, security and accountability mechanisms adequate to protect employees given the unequal bargaining relationship between employer and employee?

[5] European Parliament & Council of the European Union, 2016, Arts. 5, 28, 32 and 44; ILO, 1997; Ministry of Communications and Information Technology, 2011, Rules 6–8

1.4 Objectives of the study

1. To examine the concept, commercial rationale and operational structure of cross-border employee-data outsourcing.

2. To analyse the Indian constitutional, statutory and regulatory framework applicable to employee personal data.

3. To evaluate the allocation of responsibilities between employers, data fiduciaries, processors, vendors and sub-processors.

4. To assess the adequacy of safeguards relating to consent, transparency, security, retention, breach response and international transfers.

1.5 Scope and research methodology

This study focuses on personal data relating to employees, applicants, former employees and, where relevant, dependent beneficiaries processed in connection with employment by transnational corporations operating in or outsourcing services to India. It considers transfers to overseas affiliates, shared-service centres, cloud service providers, payroll vendors, recruitment platforms, background-verification agencies and other processors. It does not attempt a technical audit of particular corporate systems or an empirical survey of employee experiences. The analysis is doctrinal and analytical, based on legislation, constitutional principles, rules, regulatory directions, judicial decisions, policy documents and relevant comparative materials. The law must be applied with attention to commencement notifications and rules in force at the relevant date, because statutory enactment and operational commencement may occur at different times.

2. CONCEPTUAL FRAMEWORK: EMPLOYEE DATA AND CROSS-BORDER OUTSOURCING

2.1 Meaning and categories of employee data

Employee data refers broadly to information relating to an identified or identifiable individual that is collected, generated, inferred or otherwise processed in connection with recruitment, employment, workplace administration or termination. It may be supplied by the employee, obtained from public or third-party sources, generated by workplace systems, or inferred through analytics. The term covers information about current employees as well as job applicants and former employees where the information remains identifiable and is processed for employment-related purposes.[6] Common

[6] International Labour Organization [ILO], 1997; Government of India, 2023a, Section 2

categories include identity and contact data; employment and contractual records; compensation, tax and banking information; attendance and access logs; health and insurance information; biometric identifiers; performance and disciplinary records; training and skill assessments; recruitment and background-check information; workplace communications; device and network logs; and location or productivity data. Not all categories create identical risks. A work email address may present a different level of harm from a medical record, biometric template or record of disciplinary proceedings. A risk-based system should therefore consider sensitivity, volume, identifiability, context, purpose, duration and the consequences of misuse.[7]

Employee data can also become more revealing when datasets are combined. A payroll file may disclose income and financial commitments; an attendance system may reveal patterns of absence; a location system may disclose movement; and a health-benefit record may reveal medical conditions. When these datasets are linked, an employer or vendor may infer matters that were never expressly provided. Data governance must therefore address not only individual fields but also profiling, correlation, inference and secondary use.[8]

2.2 Meaning and forms of cross-border outsourcing

Cross-border outsourcing occurs where an organisation engages an entity located in another jurisdiction to perform a business function involving access to, storage of, or processing of personal data. In the employee-data context, an Indian employer may outsource payroll to a global provider, permit a foreign parent company to administer a central HR platform, use an overseas cloud environment, or engage an international analytics provider. The provider may act only on documented instructions, or it may make certain independent decisions about the means and purposes of processing. The legal character of each relationship depends on the actual functions performed rather than the contractual label alone.[9]

Several models are common. In intra-group centralisation, a parent company or regional shared-service centre processes data for subsidiaries. In third-party outsourcing, a specialist vendor performs payroll, recruitment, benefits or background verification. In cloud outsourcing, employee information is hosted on infrastructure that may be distributed across several countries. In remote-access arrangements, personnel located abroad may view or manipulate records stored in India. In software-as-a-service arrangements, the employer uses a platform operated by a vendor whose infrastructure and support teams may be geographically dispersed. Each model presents different questions about access,

[7] ILO, 1997; Government of India, 2011, Rules 2–3; Government of India, 2023a, Sections 2 and 8
[8] ILO, 1997; European Parliament & Council of the European Union, 2016, Recitals 30 and 71
[9] ILO, 1997; European Parliament & Council of the European Union, 2016, Arts. 4 and 28

transfer, control, onward disclosure and jurisdiction.

2.3 Distinction between data controller, fiduciary and processor roles

Many data-protection regimes distinguish between the organisation that determines the purposes and essential means of processing and the service provider that processes data on its behalf. Under India's DPDP framework, the statutory concepts of Data Fiduciary and Data Processor are central. The Data Fiduciary determines the purpose and means of processing, while a Data Processor processes personal data on behalf of a Data Fiduciary. In a typical employment arrangement, the employer will ordinarily determine why employee data is collected and how it is used, while payroll, cloud or HR vendors may process it under contractual instructions. However, a vendor may independently determine purposes for some activities, and the role must be assessed activity by activity.[10]The distinction matters because outsourcing does not automatically transfer the employer's legal responsibility. The employer generally remains responsible for ensuring that processing carried out on its behalf complies with applicable law, while the processor must comply with contractual and legal requirements relevant to its role. Contracts should specify permitted purposes, security controls, confidentiality, assistance with employee requests, breach notification, audit rights, deletion, retention and restrictions on sub-processing. A paper allocation of responsibility is ineffective if the actual data flows and operational controls do not match it.[11]

3. CONSTITUTIONAL AND LEGAL FOUNDATIONS OF DATA PRIVACY IN INDIA

3.1 Right to privacy under Article 21

The constitutional foundation of informational privacy in India is rooted in the right to life and personal liberty under Article 21 of the Constitution. In Justice K.S. Puttaswamy (Retd.) v. Union of India, a nine-judge Bench of the Supreme Court recognised privacy as a constitutionally protected right. The judgment treated privacy as encompassing bodily privacy, decisional autonomy and informational privacy, while recognising that the right is not absolute and may be subject to constitutionally valid restrictions. The decision is significant for employee data because it recognises that personal information and the ability to control its dissemination are closely connected with dignity and autonomy.[12]

The constitutional privacy framework requires restrictions to satisfy applicable standards of legality, legitimate State aim, necessity and proportionality. Although the direct application of

[10] ILO, 1997; European Parliament & Council of the European Union, 2016, Arts. 28 and 44–49
[11] Government of India, 2023a, Section 2(i)–(j); European Parliament & Council of the European Union, 2016, Art. 4(7)(8)
[12] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, 2017; Constitution of India, 1950, Art. 21

fundamental rights to private employers raises distinct questions, constitutional values influence statutory interpretation, public-sector employment, State action and the development of privacy norms. Where government employers or public authorities process employee data, constitutional duties may apply more directly. Private employers are primarily regulated through legislation, contracts and other applicable legal duties, but constitutional privacy principles remain an important normative foundation. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, 2017; *K.S. Puttaswamy (Aadhaar-5J.) v. Union of India*, 2018

3.2 Informational privacy, dignity and autonomy

Informational privacy is not simply secrecy. It concerns the conditions under which information about an individual is collected, used, combined, retained, shared and disclosed. Employees may reasonably expect their medical information, personal contact details, salary records and private communications to be handled differently from ordinary operational information. A workplace system that collects data for one purpose and later uses it for performance profiling or disciplinary assessment raises questions of purpose compatibility and employee autonomy.[13] The constitutional conception of dignity is also relevant. Employees should not be reduced to data points in an automated management system. Excessive biometric tracking, continuous location monitoring, intrusive productivity analytics or undisclosed profiling can affect autonomy and create a chilling effect. The law should permit legitimate workplace administration and security while requiring employers to demonstrate that intrusive processing is justified, transparent and proportionate.[14]

3.3 Information Technology Act, 2000 and associated rules

Before the DPDP framework, India's principal statutory data-protection provisions were located in the Information Technology Act, 2000, particularly Section 43A, together with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. Section 43A historically provided for compensation where a body corporate possessing, dealing with or handling sensitive personal data or information was negligent in implementing and maintaining reasonable security practices and procedures, causing wrongful loss or wrongful gain. The 2011 Rules prescribed requirements relating to privacy policies, collection, consent, purpose limitation, retention, disclosure, transfer and reasonable security practices for sensitive personal data or information.[15]

[13] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, 2017; ILO, 1997; European Parliament & Council of the European Union, 2016, Art. 5
[14] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, 2017; ILO, 1997
[15] Government of India, 2000, Section 43A; Government of India, 2011, Rules 4–8

The 2011 Rules were important in the development of Indian data-protection compliance, but their scope and structure were limited. They focused on specified categories of sensitive personal data or information and did not establish a comprehensive rights-based framework covering all forms of personal data. Their application also generated interpretive and compliance questions, particularly for complex global processing arrangements. The DPDP Act, 2023 represents a major legislative shift, although transitional and repeal provisions must be considered carefully when determining which provisions apply at a particular time.[16]

4. THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 AND EMPLOYEE DATA

4.1 Legislative purpose and scope

The Digital Personal Data Protection Act, 2023 establishes a statutory framework for processing digital personal data in India and, in specified circumstances, processing outside India in connection with offering goods or services to Data Principals in India. It seeks to recognise individuals' rights in relation to personal data while permitting lawful processing for legitimate purposes. The Act is particularly important for transnational corporations because its application is not determined solely by the location of the server. The nature of the processing, the relationship with individuals in India and the statutory territorial provisions must be considered.[17] The Act uses the concepts of Data Principal, Data Fiduciary, Data Processor, personal data and processing. An employee whose digital personal data is processed is a Data Principal. An employer that determines the purpose and means of processing may be a Data Fiduciary. A payroll or HR technology vendor may be a Data Processor where it processes data on behalf of the employer. A foreign parent company or affiliate may have a separate role depending on whether it determines purposes and means or merely performs processing under instructions. Corporate groups should map these roles rather than assume that a single global entity is responsible for every activity.[18]

4.2 Notice, consent and lawful processing

The DPDP Act generally requires processing to be undertaken in accordance with the Act and for a lawful purpose, supported by consent or a statutorily recognised legitimate use. Notice is central to transparency: individuals should be informed about the personal data to be processed and the purpose of processing, together with information relevant to the exercise of rights and the making of complaints.

[16] Government of India, 2011, Rules 2–8; Government of India, 2023a, Sections 3, 44(2); Government of India, 2025a
[17] Government of India, 2023a, Sections 3–4 and 16
[18] Government of India, 2023a, Section 2

In the employment context, notice should be specific enough to explain payroll, benefits, recruitment, attendance, security, performance management, legal compliance and any international outsourcing that materially affects the data lifecycle.[19]

The Act recognises certain legitimate uses, including specified employment-related purposes. The statutory framework includes processing for purposes related to safeguarding an employer from loss or liability, maintaining confidentiality of trade secrets, intellectual property or classified information, and providing services or benefits sought by an employee. The exact statutory conditions and the applicable version of the law must be checked when relying on these provisions. The existence of an employment-related legitimate use does not create an unlimited licence to collect any information or conduct any form of surveillance. Purpose, necessity, proportionality, security and other applicable legal requirements remain important. Consent in employment can be problematic because of the unequal bargaining position between employer and employee. A worker may formally click an acceptance box or sign a policy without having a realistic ability to refuse. This does not mean consent is always invalid, but it cautions against treating consent as a complete answer to privacy concerns. Employers should identify the correct lawful basis for each processing activity, provide clear notices, avoid bundled or misleading permissions, and distinguish mandatory employment processing from optional features such as non-essential analytics or employee-engagement applications.[20]

4.3 Duties of Data Fiduciaries

The DPDP Act places significant duties on Data Fiduciaries. These include responsibility for compliance with the Act in respect of processing undertaken by or on behalf of the Data Fiduciary, engagement of processors under a valid contract, implementation of reasonable security safeguards, and fulfilment of applicable obligations concerning personal data breaches and erasure. These duties are central to outsourcing because a Data Fiduciary cannot avoid responsibility simply by transferring operational processing to an external provider.[21]

For transnational corporations, the duty requires a governance structure that covers affiliates and vendors. The employer should understand where employee data is stored, who can access it, whether the processor uses sub-processors, what security controls are implemented and how deletion is verified. Vendor selection should include due diligence concerning technical capability, incident history, financial stability, access management, encryption, audit reports, business continuity and regulatory compliance. A contract that merely states that the vendor will comply with applicable law is insufficient

[19] Government of India, 2023a, Sections 4, 7(i) and 8; *Justice K.S. Puttaswamy (Retd.) v. Union of India*, 2017
[20] ILO, 1997; European Parliament & Council of the European Union, 2016, Recital 43 and Art. 7; Government of India, 2023a, Sections 5–6
[21] Government of India, 2023a, Section 8

if it does not translate that promise into operational controls.[22]

4.4 Data Processors and outsourcing contracts

The Act contemplates processing by a Data Processor on behalf of a Data Fiduciary under a valid contract. In employee-data outsourcing, the contract is a key instrument for allocating operational responsibilities. It should define the subject matter and duration of processing, categories of data and individuals, permitted purposes, instructions, confidentiality requirements, security safeguards, incident reporting, assistance with rights requests, audit and inspection, sub-processor approval, international access, return or deletion of data, and cooperation with regulators.[23]

A processor should not use employee information for independent advertising, unrelated product development, unauthorised model training or commercial profiling unless a separate lawful basis and appropriate transparency exist. The contract should prohibit unauthorised onward disclosure and require equivalent obligations to flow down to sub-processors. It should also establish practical response times, evidence preservation, cooperation during investigations and a clear process for termination and secure deletion. Where the provider is part of the same corporate group, the absence of an external commercial contract does not eliminate the need for documented governance and clear allocation of roles.[24]

5. CROSS-BORDER TRANSFERS UNDER INDIAN LAW

5.1 The statutory approach to international transfers

Cross-border transfer is one of the central issues in the DPDP framework. The Act adopts a model under which personal data may be transferred outside India, subject to restrictions that the Central Government may impose by notification in respect of specified countries or territories and to any other applicable Indian law that provides a higher degree of protection or imposes restrictions. This approach differs from a general rule that all personal data must remain within India. It provides a conditional transfer framework while retaining governmental authority to restrict transfers to specified destinations.[25]

For transnational corporations, the practical effect is that a transfer assessment cannot be based on a general assumption that overseas processing is either always prohibited or always permitted. Organisations must monitor the current notifications and rules, identify the destination jurisdictions and

[22] Government of India, 2023a, Section 8; European Parliament & Council of the European Union, 2016, Arts. 28 and 32; ILO, 1997
[23] Government of India, 2023a, Section 8(2); European Parliament & Council of the European Union, 2016, Art. 28
[24] Government of India, 2023a, Sections 4, 8 and 12; European Parliament & Council of the European Union, 2016, Arts. 5, 28 and 32; ILO, 1997
[25] Government of India, 2023, Section 16; Government of India, 2025a, G.S.R. 843(E)

recipients, and determine whether sector-specific or other legal requirements impose additional conditions. The location of the primary data centre may not tell the whole story: remote support access, disaster-recovery replication, analytics, technical troubleshooting and onward transfers can also involve processing outside India.[26]

5.2 Data localisation and sector-specific requirements

Data localisation refers to legal or policy requirements that data be stored or processed within a particular jurisdiction. The DPDP Act does not establish a universal localisation requirement for all personal data. However, other Indian laws, regulatory directions and sectoral frameworks may impose localisation or storage requirements for specified categories of data or regulated entities. For example, financial-sector entities, payment system operators, regulated intermediaries and certain telecommunications or critical infrastructure actors may be subject to distinct requirements. The precise applicability depends on the entity, data category, service and relevant regulator.[27]

Transnational corporations should therefore conduct a sectoral mapping exercise before moving employee data to global platforms. A bank, payment system participant, insurance entity, telecom provider or critical information infrastructure operator may have obligations beyond the general DPDP transfer framework. Employment data can also be embedded in operational systems containing customer, financial or regulated business information. The organisation should distinguish employee records from other regulated datasets while ensuring that shared systems do not create accidental non-compliance.

5.3 Onward transfers and supply-chain complexity

A cross-border transfer rarely ends with the first recipient. A global HR provider may use a cloud hosting company, which may engage a security monitoring vendor, which may rely on a support team in another jurisdiction. A payroll processor may use a local bank, tax platform or identity verification service. Each additional participant increases the number of entities with potential access to employee data and expands the attack surface. It also complicates the identification of the entity responsible for a breach or unauthorised use.[28]

Contracts should require prior authorisation or clearly defined conditions for sub-processing,

[26] Government of India, 2011, Rule 7; European Parliament & Council of the European Union, 2016, Arts. 44–49; Information Commissioner's Office [ICO], 2026
[27] Government of India, 2023, Section 16; Reserve Bank of India [RBI], 2018; Securities and Exchange Board of India [SEBI], 2023
[28] European Parliament & Council of the European Union, 2016, Arts. 28 and 44; International Labour Organization [ILO], 1997

transparency about locations and recipients, equivalent security and confidentiality obligations, and responsibility for the acts and omissions of sub-processors. Organisations should maintain a current register of processors and sub-processors, including the categories of data accessed, processing locations, support locations and onward-transfer routes. A one-time vendor assessment is insufficient where the supply chain changes over time.[29]

6. INFORMATION SECURITY RISKS IN CROSS-BORDER EMPLOYEE-DATA OUTSOURCING

6.1 Nature of information-security threats

Employee data is an attractive target for cybercriminals because it may contain identity credentials, financial details, tax identifiers, health information and access credentials that can be exploited for fraud, identity theft, phishing, extortion or corporate espionage. Outsourcing increases the number of systems, users and organisations that may access the information. Threats include ransomware, credential theft, phishing, insider misuse, misconfigured cloud storage, insecure APIs, unpatched systems, supply-chain compromise, data exfiltration and accidental disclosure.[30]

The risk is not limited to sophisticated external attacks. A vendor employee may download a payroll file to an unmanaged device; a support engineer may access records without a valid business need; a misconfigured access permission may expose a database; or a departing contractor may retain credentials. The security framework must therefore address human, technical and organisational risks. It should be designed around the actual data lifecycle and not merely the existence of a cybersecurity policy.[31]

6.2 Reasonable security safeguards

Reasonable security safeguards should be proportionate to the nature, volume and sensitivity of employee data and the likely consequences of compromise. Core measures include encryption in transit and at rest, strong authentication, role-based access control, privileged-access management, network segmentation, secure configuration, vulnerability management, endpoint protection, secure software development, logging, monitoring, backup protection and tested recovery procedures. Sensitive fields

[29] European Parliament & Council of the European Union, 2016, Arts. 28 and 32; Government of India, 2011, Rules 6–8; ILO, 1997
[30] ILO, 1997; Indian Computer Emergency Response Team [CERT-In], 2022; European Parliament & Council of the European Union, 2016, Art. 32
[31] CERT-In, 2022; Government of India, 2011, Rule 8; ILO, 1997

should be masked or tokenised where full values are not required for a task.[32]

Technical controls must be supported by organisational measures. These include security policies, staff training, confidentiality undertakings, background checks where lawful and proportionate, incident-response plans, vendor due diligence, periodic audits, access reviews, business continuity planning and documented accountability. Access should follow the principle of least privilege: a payroll processor should not automatically receive access to medical or disciplinary records, and a global administrator should not have unrestricted access merely because a system is technically centralised.[33]

6.3 Encryption, pseudonymisation and access controls

Encryption reduces the risk that data can be understood if storage media or communications are intercepted, although it does not prevent misuse by authorised users who possess decryption keys. Key management is therefore critical. Organisations should separate key administration from ordinary system administration, rotate keys according to risk, monitor access and ensure that backups are protected. Pseudonymisation can reduce exposure by replacing direct identifiers with codes, but re-identification may remain possible where additional information is available. It should not be treated as equivalent to anonymisation.[34]

Access controls should be granular and reviewed regularly. Multi-factor authentication should be used for privileged and remote access. Administrative sessions should be logged and, for high-risk systems, monitored. Access should be time-limited where possible, and emergency access should be subject to additional controls and post-event review. These measures are particularly important where overseas personnel provide technical support or administer a global HR platform.[35]

7. EMPLOYMENT LAW, CONSENT AND WORKPLACE AUTONOMY

7.1 Employment contracts and privacy notices

Employment contracts commonly authorise the employer to collect information necessary for recruitment, payroll, benefits, compliance and workplace administration. Separate policies may address IT usage, confidentiality, monitoring, security and data protection. These documents should be consistent and should not rely on broad clauses that purport to authorise every possible use of employee information. A clear privacy notice should explain the categories of information, purposes, recipients,

[32] CERT-In, 2022; Government of India, 2011, Rule 8; European Parliament & Council of the European Union, 2016, Art. 32
[33] CERT-In, 2022; ILO, 1997; European Parliament & Council of the European Union, 2016, Arts. 28 and 32
[34] European Parliament & Council of the European Union, 2016, Arts. 4(5), 25 and 32; ILO, 1997
[35] CERT-In, 2022; European Parliament & Council of the European Union, 2016, Arts. 25 and 32

international transfers, retention periods, employee rights and grievance channels.

The notice should distinguish mandatory processing from optional processing. For example, bank details may be necessary for salary payment, while participation in a non-essential employee-engagement application may be optional. Biometric attendance may be justified in some circumstances, but the employer should consider whether less intrusive methods are available and whether the system is proportionate. The mere fact that a technology is widely used by other employers does not establish that it is necessary or lawful in every workplace.[36]

7.2 Power imbalance and meaningful choice

A worker may have little practical ability to negotiate the terms of data processing. Refusal to provide information may result in an inability to receive salary, access workplace systems or obtain statutory benefits. This power imbalance requires employers to be cautious when relying on consent. Consent should be specific, informed and freely given where the law requires it. Where processing is necessary for employment-related purposes recognised by law, the employer should rely on the relevant legal basis and explain it transparently rather than obtaining unnecessarily broad consent.[37]

The principle of data minimisation is particularly important. Employers should collect only information reasonably required for an identified purpose and should not retain it indefinitely. A request for health information should be limited to what is necessary for a specific occupational or benefits purpose. Background checks should be relevant to the role and comply with applicable law. Monitoring should be tailored to a genuine business or security need and should not be used to collect unrelated personal information.

7.3 Automated decision-making and employee profiling

Global HR platforms increasingly use analytics to rank candidates, assess performance, predict attrition, allocate shifts, identify training needs or flag potential misconduct. Such systems may process employee data across borders and may generate inferences that affect promotion, remuneration, discipline or termination. Even where a system does not make the final decision, its outputs may influence managers and create a risk of automation bias.[38]

Organisations should assess the accuracy, relevance and fairness of data used in employment

[36] ILO, 1997; Government of India, 2011, Rules 4–5; European Parliament & Council of the European Union, 2016, Arts. 5 and 13
[37] ILO, 1997; European Parliament & Council of the European Union, 2016, Recital 43 and Art. 7; Government of India, 2023, Section 7(i)
[38] ILO, 1997; European Parliament & Council of the European Union, 2016, Arts. 22 and 35

analytics. Employees should have an appropriate channel to challenge inaccurate information and seek human review where consequential decisions are affected. Models should be tested for discriminatory outcomes, proxy variables and systematic errors. The employer should also understand whether the vendor uses employee data to train or improve models for other customers. Contractual restrictions and transparency are essential where the data is reused for product development or artificial intelligence systems.[39]

8. REGULATORY AND INSTITUTIONAL CHALLENGES IN INDIA

8.1 Fragmented regulatory landscape

Employee-data governance may involve the data-protection framework, information technology law, cybersecurity directions, employment statutes, tax and social-security obligations, sectoral regulation, contractual duties and constitutional principles. Different regulators may oversee different aspects of the same corporate activity. A company may be subject to data-protection obligations as a Data Fiduciary, cybersecurity requirements as a regulated entity or service provider, and employment obligations as an employer. The challenge is to identify overlapping requirements and avoid gaps in responsibility.[40]

The DPDP framework provides a general statutory architecture, but it does not displace every sector-specific rule. Nor does it eliminate the need to comply with employment, tax, corporate, financial and cybersecurity requirements. Organisations should maintain a legal obligations register that identifies the relevant regulator, data category, processing activity, transfer restriction, retention period, incident-reporting duty and responsible internal function. This is particularly important for groups operating in regulated sectors.[41]

8.2 Role of the Data Protection Board

The DPDP Act provides for the Data Protection Board of India as the statutory body responsible for performing functions assigned under the Act, including inquiry and enforcement functions in accordance with the statutory framework. Its effectiveness will depend on institutional capacity, procedural clarity, technical expertise, independence in decision-making and the ability to address complex cross-border processing arrangements. Employee complaints may involve technical questions about access logs, vendor relationships, data flows and international transfers that require specialised

[39] European Parliament & Council of the European Union, 2016, Arts. 5, 22 and 35; ILO, 1997; Government of India, 2023, Sections 8 and 12
[40] Government of India, 2000, Sections 43A and 70B; Government of India, 2011; CERT-In, 2022; RBI, 2018; SEBI, 2023
[41] Government of India, 2023, Sections 16 and 44; RBI, 2018; SEBI, 2023; CERT-In, 2022

understanding.[42]

The Board's procedures and the commencement of relevant provisions should be assessed by reference to current notifications and rules. Organisations should not assume that all provisions became operational on the date the Act received assent. Equally, they should not treat phased commencement as a reason to postpone compliance planning. Large employers and service providers require time to map systems, revise contracts, train personnel and build response capabilities.[43]

8.3 Enforcement across corporate groups and foreign vendors

Enforcement becomes more difficult when a foreign processor or sub-processor has no substantial presence in India, stores information abroad or operates through multiple affiliates. The Indian employer may remain the most accessible point of accountability, but it may lack direct control over the foreign vendor's infrastructure. Contractual audit rights, cooperation obligations and data-return provisions are therefore essential. Regulatory cooperation between jurisdictions may also be necessary where evidence, personnel or servers are located abroad.[44]

A corporate group should not rely solely on the assumption that a foreign parent company will voluntarily comply with Indian requirements. It should document the legal basis for group-wide access, identify the entity responsible for each processing activity, ensure that access is limited, and maintain escalation routes for Indian employees and regulators. Where a foreign affiliate independently determines purposes and means, it may have obligations in its own capacity rather than merely acting as a processor.[45]

9. COMPARATIVE PERSPECTIVES

9.1 European Union: GDPR and international transfers

The European Union's General Data Protection Regulation provides a comprehensive framework for personal data processing, including employment-related data where national law and collective arrangements may supplement the Regulation. It establishes principles such as lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality and accountability. It also distinguishes controllers and processors and imposes

[42] Government of India, 2023, Sections 18–26; Government of India, 2025b, G.S.R. 844(E) and G.S.R. 845(E)
[43] Government of India, 2025a, G.S.R. 843(E); Government of India, 2025c, G.S.R. 846(E)
[44] European Parliament & Council of the European Union, 2016, Arts. 28 and 44–49; Government of India, 2023, Sections 8 and 16; ILO, 1997
[45] Government of India, 2023, Sections 2 and 8; European Parliament & Council of the European Union, 2016, Arts. 4 and 28

contractual and security obligations on processors.[46]

The GDPR regulates transfers of personal data to third countries through mechanisms including adequacy decisions, appropriate safeguards such as standard contractual clauses, and specified derogations. This system illustrates a structured approach in which transfer permissibility is linked to protection and enforceable safeguards. It also demonstrates that cross-border transfers require more than a generic contractual promise: organisations must consider the legal environment of the destination, onward access and practical enforceability. India's framework is different in design, but the European experience offers useful lessons on accountability, documentation, processor contracts and transfer risk assessment.[47]

9.2 United Kingdom and other approaches

The United Kingdom's data-protection framework, based on the UK GDPR and Data Protection Act 2018 as amended, also regulates international transfers through adequacy regulations and appropriate safeguards. Other jurisdictions adopt different models, including localisation requirements, government-approved transfer mechanisms, contractual protections or sector-specific restrictions. These differences create compliance complexity for multinational employers whose global HR systems must serve employees in many countries.[48]

No single foreign model can simply be transplanted into India. The appropriate framework must account for India's constitutional structure, digital economy, regulatory capacity, employment practices, public-sector role and international trade interests. Comparative analysis is most useful when it identifies practical safeguards that can be adapted, rather than treating another jurisdiction's legal architecture as inherently superior.[49]

9.3 Lessons for India

India can draw several lessons from comparative practice: clear allocation of controller and processor roles; detailed processor contracts; transparent notices; risk assessments for high-impact processing; robust security safeguards; meaningful transfer controls; and accessible remedies. It may also consider more specific guidance for employee data, given the power imbalance and the sensitive nature of workplace monitoring. Such guidance could explain when processing is necessary for employment, how consent should be treated, and what safeguards should apply to biometric systems,

[46] European Parliament & Council of the European Union, 2016, Arts. 5, 24, 28 and 32
[47] European Parliament & Council of the European Union, 2016, Arts. 44–49; European Commission, 2021
[48] Data Protection Act 2018, Sections 73–75; ICO, 2026
[49] ILO, 1997; European Parliament & Council of the European Union, 2016; Government of India, 2023

location tracking and automated HR analytics.[50]

10. CRITICAL ANALYSIS

10.1 Adequacy of the DPDP framework for employee data

The DPDP Act provides a significant improvement over the earlier fragmented approach by creating a general framework for digital personal data, recognising individual rights and imposing duties on Data Fiduciaries. Its application to employer-led processing and outsourced services can support accountability across the processing chain. The recognition of Data Processors and the requirement for valid contracts are particularly relevant to payroll providers, HR platforms and cloud vendors. The transfer framework also avoids a blanket localisation rule while preserving the ability of the Government to restrict specified destinations.[51]

Nevertheless, the framework leaves practical questions that are particularly important in employment. The Act does not establish a separate, comprehensive code for employee data. Employment-related legitimate uses may facilitate necessary processing, but their scope must not be interpreted as a general exemption from privacy and security principles. Employees may not have meaningful bargaining power, and broad internal policies may obscure the actual extent of global data sharing. Guidance is therefore required to distinguish necessary employment administration from excessive monitoring or secondary commercial use.[52]

10.2 Limits of consent as the primary safeguard

Consent is often presented as the foundation of data protection, but its practical value is limited where an employee cannot realistically refuse. A new employee may sign multiple documents without understanding that data will be hosted overseas, accessed by global support teams or analysed by an external provider. Even where the legal basis is not consent, transparency remains necessary. Employers should not use the existence of a consent clause to avoid explaining processing purposes or assessing necessity.[53]

A better model combines an appropriate legal basis with employee-facing transparency, purpose limitation, minimisation, security and grievance mechanisms. For optional processing, employees should have a genuine choice without adverse consequences. For necessary employment processing,

[50] ILO, 1997; European Parliament & Council of the European Union, 2016, Arts. 5, 28, 32 and 35; ICO, 2026
[51] Government of India, 2023, Sections 2, 8 and 16; Government of India, 2011, Rules 6–8
[52] Government of India, 2023, Sections 7(i) and 8; ILO, 1997; *Justice K.S. Puttaswamy (Retd.) v. Union of India*, 2017
[53] ILO, 1997; European Parliament & Council of the European Union, 2016, Recital 43 and Art. 7

the employer should explain the legal and operational basis and collect only what is required. This approach recognises the realities of employment without reducing employees to passive subjects of corporate data systems.[54]

10.3 The gap between contractual compliance and actual security

Outsourcing contracts frequently contain confidentiality and security clauses, but contractual language does not guarantee that systems are secure. A vendor may promise encryption but fail to manage keys; it may promise access control but permit excessive administrator privileges; or it may promise prompt incident reporting but lack effective detection. Compliance should therefore be verified through risk-based due diligence, independent assessments, audit rights, penetration testing where appropriate, incident simulations and ongoing monitoring.[55]

The employer must also retain sufficient expertise to supervise the processor. Outsourcing should not mean outsourcing accountability. If the employer cannot understand the data flows, security architecture or incident response arrangements of its vendor, it may be unable to demonstrate meaningful governance. This is especially important where a global provider uses multiple sub-processors or changes its hosting locations over time.

10.4 Balancing business efficiency and employee rights

The case for cross-border outsourcing is substantial. Shared services can reduce administrative cost, improve payroll accuracy, provide specialist security and support global workforce management. Excessive restrictions may fragment systems, increase costs and undermine the competitiveness of Indian businesses. However, efficiency must be achieved through lawful and secure processing. Employees should not bear disproportionate privacy and security risks merely because a corporation seeks to centralise operations.[56]

A balanced approach is risk-based. Low-risk administrative information may be processed through standard contractual and security controls, while highly sensitive information such as health, biometric or disciplinary records should receive stronger access restrictions, minimisation, encryption and review. High-impact monitoring and profiling should be subject to a documented necessity assessment and human oversight. The law should encourage secure and responsible outsourcing rather than prohibit

[54] ILO, 1997; Government of India, 2023, Sections 5–8; European Parliament & Council of the European Union, 2016, Arts. 5–7
[55] CERT-In, 2022; European Parliament & Council of the European Union, 2016, Arts. 28 and 32; ILO, 1997
[56] ILO, 1997; European Parliament & Council of the European Union, 2016, Recitals 5–6; Government of India, 2023

legitimate international business models.

11. RECOMMENDATIONS

11.1 Issue specific guidance on employee personal data

The competent authorities should consider issuing practical guidance on employment-related processing under the DPDP framework. Guidance should address recruitment, payroll, benefits, background checks, attendance, biometric systems, workplace monitoring, HR analytics, former-employee records and international transfers. It should explain the distinction between necessary employment processing and optional or secondary uses, and clarify the safeguards expected where employees have limited bargaining power.[57]

11.2 Require robust data mapping and transfer assessments

Transnational corporations should maintain an up-to-date map of employee-data flows, including collection points, storage locations, remote access, recipients, sub-processors, retention periods and deletion processes. Before transferring data, organisations should identify the destination, purpose, applicable restrictions, onward-transfer risks and security controls. This assessment should be revisited when a vendor, hosting location, processing purpose or applicable law changes.[58]

11.3 Strengthen processor and sub-processor contracts

Outsourcing agreements should contain detailed clauses on processing instructions, confidentiality, security, incident reporting, audit, assistance with employee rights, sub-processing, international access, retention, deletion and regulatory cooperation. The employer should retain approval rights or effective controls over material sub-processors. Contracts should require the processor to notify the employer of changes to data locations or material security arrangements and to provide evidence of compliance.[59]

11.4 Adopt risk-based security controls

Employers and vendors should implement encryption, tokenisation where appropriate, multi-factor authentication, role-based access, privileged-access management, logging, vulnerability management, secure backups and tested incident response. Access to health, biometric and disciplinary records should

[57] ILO, 1997; Government of India, 2023, Sections 7 and 8; European Parliament & Council of the European Union, 2016, Arts. 5 and 6
[58] European Parliament & Council of the European Union, 2016, Arts. 30 and 44–49; ICO, 2026; Government of India, 2011, Rule 7
[59] European Parliament & Council of the European Union, 2016, Arts. 28 and 32; Government of India, 2023, Section 8; ILO, 1997

be particularly restricted. Organisations should also conduct regular access reviews and ensure that accounts are promptly disabled when employees or vendor personnel leave or change roles.[60]

11.5 Improve breach response and employee communication

A unified incident-response framework should require vendors to report suspected incidents promptly, preserve evidence and cooperate with investigation. Employers should identify the applicable statutory notification requirements and communicate with affected employees in a clear and timely manner where required. Communications should explain the type of information affected, likely consequences, protective steps and available grievance channels. Lessons from incidents should be incorporated into vendor oversight and system design.[61]

12. CONCLUSION

Cross-border outsourcing of employee data has become an integral part of transnational corporate operations. Global payroll systems, centralised HR platforms, cloud computing, remote technical support and specialist service providers allow businesses to administer a geographically dispersed workforce efficiently. Yet, these arrangements also expose employees to risks that are difficult to address through traditional employment contracts alone. Employee data may contain identity, financial, health, biometric, performance and behavioural information. Its movement across multiple entities and jurisdictions creates challenges concerning transparency, accountability, security, retention, onward disclosure and effective remedies.[62]

India's legal framework has undergone a significant transition. Constitutional privacy principles, particularly as recognised in Puttaswamy, provide a normative foundation for informational privacy and dignity. The Information Technology Act, 2000 and the 2011 SPDI Rules formed an earlier statutory framework, while the Digital Personal Data Protection Act, 2023 establishes a broader model based on Data Principals, Data Fiduciaries, Data Processors, lawful processing, security safeguards, rights and conditional cross-border transfers. The framework is relevant to transnational corporations because outsourcing does not, by itself, remove the employer's responsibility for processing carried out on its behalf.[63] The DPDP framework offers an important foundation, but the practical protection of employees depends on implementation. Employment-related processing may be necessary for payroll,

[60] CERT-In, 2022; European Parliament & Council of the European Union, 2016, Art. 32; Government of India, 2011, Rule 8
[61] CERT-In, 2022; Government of India, 2000, Section 70B; European Parliament & Council of the European Union, 2016, Arts. 33–34; Government of India, 2023, Section 8(6)
[62] ILO, 1997; European Parliament & Council of the European Union, 2016; CERT-In, 2022
[63] (*Justice K.S. Puttaswamy (Retd.) v. Union of India*, 2017; Government of India, 2000; Government of India, 2011; Government of India, 2023, Sections 2, 8 and 16)

benefits, security and administration, yet the power imbalance between employer and employee makes consent an imperfect safeguard. Broad privacy notices and generic vendor contracts cannot replace meaningful transparency, data minimisation, access controls, processor oversight and effective grievance mechanisms. The cross-border nature of outsourcing further requires organisations to identify destination jurisdictions, remote access, sub-processors and applicable sectoral restrictions.[64]

Information security must be treated as a continuous governance obligation. Encryption, access management, monitoring, vulnerability management, incident response, vendor audits and deletion controls should operate throughout the data lifecycle. At the same time, security measures must not become a justification for disproportionate workplace surveillance. Employee monitoring and automated HR analytics should be limited to legitimate purposes, proportionate to the risk and open to appropriate review. Employees must be able to understand how their information is used and how they can raise concerns.[65] The appropriate policy response is neither an absolute prohibition on international outsourcing nor unrestricted corporate freedom to move employee information. India should pursue a risk-based model that enables legitimate business operations while ensuring that employee privacy and information security remain central. Specific guidance on employment data, clear processor obligations, robust transfer assessments, effective breach response, protection against excessive monitoring and stronger regulatory coordination would improve the framework. Ultimately, responsible cross-border outsourcing depends on a simple principle: the geographical movement of employee data must not dilute the legal responsibility owed to the individual to whom that data relates.[66]

[64] ILO, 1997; Government of India, 2023, Sections 5–8 and 16; European Parliament & Council of the European Union, 2016, Arts. 5, 7 and 28

[65] CERT-In, 2022; ILO, 1997; European Parliament & Council of the European Union, 2016, Arts. 5, 22, 25 and 32

[66] ILO, 1997; Government of India, 2023, Sections 8 and 16; European Parliament & Council of the European Union, 2016, Arts. 28, 32 and 44–49

REFERENCES:

A. Indian Constitutional and Legislative Sources

- Government of India. (1950). *The Constitution of India.* Legislative Department, Ministry of Law and Justice.

- Government of India. (2000). *The Information Technology Act, 2000 (Act No. 21 of 2000).*

- Government of India. (2011). *The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.* Ministry of Communications and Information Technology.

- Government of India. (2023). *The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).* Ministry of Electronics and Information Technology.

B. DPDP Act, 2023 – Government Notifications and Rules

- Government of India. (2025a). *Notification G.S.R. 843(E): Commencement of provisions of the Digital Personal Data Protection Act, 2023.* Ministry of Electronics and Information Technology, Gazette of India, 13 November 2025.

- Government of India. (2025b). *Notification G.S.R. 844(E): Establishment of the Data Protection Board of India.* Ministry of Electronics and Information Technology, Gazette of India, 13 November 2025.

- Government of India. (2025c). *Notification G.S.R. 845(E): Composition of the Data Protection Board of India.* Ministry of Electronics and Information Technology, Gazette of India, 13 November 2025.

- Government of India. (2025d). *The Digital Personal Data Protection Rules, 2025 (G.S.R. 846(E)).* Ministry of Electronics and Information Technology, Gazette of India, 13 November 2025.

C. Indian Regulatory Directions and Circulars

- Indian Computer Emergency Response Team. (2022). *Directions relating to information security practices, procedure, prevention, response and reporting of cyber incidents for safe and trusted internet.* Ministry of Electronics and Information Technology, Government of India.

- Reserve Bank of India. (2018, April 6). *Storage of payment system data* (RBI/2017-18/153; DPSS.CO.OD No. 2785/06.08.005/2017-2018).

- Securities and Exchange Board of India. (2023, March 6). *Framework for adoption of cloud services by SEBI regulated entities (REs)* (Circular No. SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033).

D. International Regulations and Legal Instruments

- European Parliament & Council of the European Union. (2016). *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 (General Data Protection Regulation).* Official Journal of the European Union, L 119, 1–88.

- European Commission. (2021). *Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679.* Official Journal of the European Union, L 199, 31–61.

- United Kingdom. (2018). *Data Protection Act 2018.*

E. International Labour Standards and Institutional Publications

- International Labour Organization. (1997). *Protection of workers' personal data: ILO code of practice.* International Labour Office.

- Information Commissioner's Office. (2026). *A guide to international transfers.*

- Information Commissioner's Office. (2026). *Appropriate safeguards.*