The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2025

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

EMPLOYEE DATA AND PRIVACY LAWS: HR PRACTICES IN TRANSITION

Gautam Mehra

ABSTRACT

The digital transformation of Human Resources has led to an exponential increase in the collection and processing of employee personal data, necessitating robust legal and ethical frameworks. This paper examines the evolving landscape of employee data privacy, focusing on the impact of global regulations such as the EU's General Data Protection Regulation (GDPR), the California Privacy Rights Act (CPRA) in the U.S., and India's Digital Personal Data Protection Act, 2023 (DPDP Act). It argues that the convergence of these stringent privacy norms with advanced digital technologies, particularly cloud computing and Artificial Intelligence, demands a fundamental shift in HR practices towards privacy-by-design principles. The paper delves into core data protection principles, specific provisions of the DPDP Act, and the implications of GDPR and CPRA for employment data. Through an analysis of key HR functions (recruitment, performance management, employee monitoring) and the challenges posed by digital transformation, cloud computing, and AI (including bias and transparency issues), it highlights essential mitigation strategies. Case studies illustrate the real-world consequences of non-compliance. Ultimately, the paper concludes that proactive data governance, comprehensive data mapping, clear policies, continuous training, rigorous vendor due diligence, and embedding privacy by design are crucial for HR to effectively leverage data while upholding privacy, fostering trust, and mitigating significant legal and reputational risks.

I. INTRODUCTION: THE EVOLVING LANDSCAPE OF EMPLOYEE DATA PRIVACY

The digital age has fundamentally transformed how organizations operate, with data becoming an indispensable asset, particularly within Human Resources. From initial recruitment to ongoing performance management, businesses extensively collect, process, and store vast amounts of employee personal information. This increasing reliance on data, coupled with its growing volume and sensitivity, necessitates robust legal and ethical frameworks to prevent misuse, unauthorized access, and data breaches. The digital transformation of HR, encompassing advanced applicant tracking systems, cloud-based payroll solutions, and sophisticated AI-driven analytics, further amplifies the complexity of responsible data management. This evolution demands a proactive approach to data governance, moving beyond mere compliance to embed privacy as a core organizational value.[1] Historically, employee information was predominantly managed through physical files, with limited and controlled access. However, digital technologies have revolutionized this, leading to the routine electronic collection, storage, and processing of employee data across diverse platforms and systems, often spanning multiple jurisdictions. This includes personal identifiers, contact information, employment history, performance reviews, health records, biometric data, financial details, and data derived from employee monitoring. While this interconnectedness offers unprecedented opportunities for efficiency and insights, it simultaneously presents significant challenges in maintaining security, privacy, and regulatory adherence.[2]

Globally, data protection laws have matured considerably, establishing new benchmarks for organizational accountability and individual rights. The European Union's General Data Protection Regulation (GDPR),[3] enacted in 2018, set a comprehensive and stringent framework that has profoundly influenced legislation worldwide. Its principles of accountability, transparency, and data subject rights have become a de facto global standard. In the United States, the California Consumer Privacy Act (CCPA), significantly amended by the California Privacy Rights Act (CPRA), has introduced robust protections, notably extending comprehensive consumer privacy rights to employee data within California. This

---

[1] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, INDIA CODE (2023).

[2] India's Digital Personal Data Protection Act, 2023: An Overview, NISHITH DESAI ASSOCIATES (Aug. 11, 2023), https://www.nishithdesai.com/SectionLanding/37/26/Nishith-Desai-Associates/Research-and-Articles/Research-Papers/Research-Papers.html?id=4842.

[3] What are the GDPR principles?, GDPR.EU (last visited July 18, 2025), https://gdpr.eu/gdpr-principles/.

mandates that businesses operating in California afford their employees similar control over their personal information as their customers. More recently, India's Digital Personal Data Protection Act, 2023 (DPDP Act), enacted on August 11, 2023, marks a pivotal step in India's data governance journey. This Act establishes a comprehensive framework for digital personal data protection, aiming to balance individual rights with legitimate business needs for data processing, thereby positioning India as a significant player in global data governance and influencing multinational corporations operating in the region.[4]

This paper argues that the convergence of increasingly stringent global privacy norms and the advent of sophisticated digital technologies, particularly Artificial Intelligence (AI) and pervasive cloud computing solutions, necessitates a fundamental transformation in HR practices. Organizations must transcend traditional, reactive compliance to embed privacy-by-design principles into every facet of their HR operations. This proactive stance is crucial not only for ensuring ethical data handling and fostering employee trust but also for mitigating substantial legal liabilities, significant financial penalties, and severe reputational risks in this rapidly evolving landscape. The transition requires a holistic approach, integrating legal compliance with technological safeguards and cultivating a pervasive culture of privacy awareness throughout the entire organization.

II. FOUNDATIONAL PRINCIPLES OF DATA PROTECTION IN EMPLOYMENT

The global landscape of data privacy laws, including GDPR, DPDP Act, and CCPA/CPRA, is built upon a set of core data protection principles. Adherence to these principles is fundamental for lawful and ethical data processing, ensuring individual privacy rights are respected throughout the data lifecycle.[5]

Core Data Protection Principles

- Lawfulness, Fairness, and Transparency: Personal data processing must be lawful, fair, and transparent.[6]

[4] Employee Monitoring and Data Protection, ICO (Information Commissioner's Office) (last visited July 18, 2025), https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/employee-monitoring-and-data-protection/.
[5] GDPR and Recruitment: A Comprehensive Guide, WORKABLE (last visited July 18, 2025), https://resources.workable.com/tutorial/gdpr-recruitment-guide
[6] What is GDPR, the EU's data protection law?, IBM (last visited July 18, 2025), https://www.ibm.com/topics/gdpr.

    - Lawfulness: Requires a valid legal basis (e.g., consent, contract, legal obligation, legitimate interests).
    - Fairness: Processing must align with data subjects' expectations and interests.
    - Transparency: Demands clear communication about data collection, processing, and purpose.
- Purpose Limitation: Data must be collected for specified, explicit, and legitimate purposes and not processed incompatibly with those purposes.
- Data Minimisation: Collected data must be adequate, relevant, and strictly limited to what is necessary for its purpose.
- Accuracy: Personal data must be accurate, kept up-to-date, and regularly reviewed.
- Storage Limitations: Data should be deleted once no longer needed for its original purpose, unless legally required for retention.
- Integrity and Confidentiality: Data must be secured against unauthorized processing, loss, destruction, or damage through technical and organizational measures (e.g., encryption, access controls).
- Accountability: The data controller (employer) must demonstrate compliance with these principles.[7]

DEFINITION AND SIGNIFICANCE OF PERSONAL DATA AND SENSITIVE PERSONAL DATA[8]

- Personal Data (PI): Any information identifying an individual directly or indirectly. In employment, this includes names, contact info, employment history, performance reviews, and inferences.[9]
- Sensitive Personal Data (SPD/SPII): A subset of personal data whose unauthorized disclosure could cause significant harm or discrimination.
    - GDPR: Includes racial/ethnic origin, political opinions, religious beliefs, trade-union membership, genetic, biometric, health, and sexual orientation data.

---

[7] DPDP Act 2023: Impact on the Employment Sector, CYBER LAW CONSULTING (Sept. 1, 2023), https://cyberlawconsulting.com/dpdp-act-2023-impact-on-the-employment-sector/.
[8] What is Sensitive Personal Information (SPI)?, TECHTARGET (last visited July 18, 2025), https://www.techtarget.com/searchsecurity/definition/Sensitive-Personal-Information-SPI.
[9] Impact of DPDP Act, 2023 on Employers, KHAITAN & CO. (Sept. 15, 2023), https://www.khaitanco.com/insights/impact-of-dpdp-act-2023-on-employers.

- CCPA/CPRA: Adds social security numbers, financial credentials, precise geolocation, and citizenship status. SPD is subject to stricter processing conditions and heightened security, carrying higher legal and reputational risks.

UNIVERSAL FOUNDATIONAL PILLARS OF DATA PROTECTION

The consistent presence of principles like lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability across GDPR, DPDP Act, and CCPA/CPRA signifies a global consensus on responsible data stewardship. This convergence simplifies foundational compliance for multinational organizations, though specific implementation and enforcement vary by jurisdiction.[10]

III. INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT, 2023: A DEEP DIVE[11]

India's DPDP Act, 2023, enacted on August 11, 2023, establishes a robust framework for data privacy.

A. KEY DEFINITIONS AND APPLICABILITY

- Data Principal: The individual to whom personal data relates (e.g., an employee).
- Data Fiduciary: Determines the purpose and means of processing personal data (e.g., the employer).
- Data Processor: Processes personal data on behalf of a Data Fiduciary (e.g., a payroll service provider). The Data Fiduciary remains accountable and must have a contract with the Processor.
- Significant Data Fiduciary (SDF): Classified by the Central Government based on data volume/sensitivity and risk. SDFs face more stringent compliance obligations.

[10] GDPR Fines and Penalties: A Comprehensive Guide, VEEAM (last visited July 18, 2025), https://www.veeam.com/blog/gdpr-fines-penalties.html.
[11] India's DPDP Act, 2023 and the Employment Sector, PEOPLE MATTERS (Sept. 29, 2023), https://www.peoplemattersglobal.com/article/compliance/indias-dpdp-act-2023-and-the-employment-sector-39659.

The Act applies to digital personal data processed within India or outside India if processing is for offering goods/services to Indian individuals.[12]

B. LAWFUL BASIS FOR PROCESSING EMPLOYEE DATA

Consent Requirements -

Generally, personal data processing requires explicit consent: "free, specific, informed, unconditional and unambiguous with a clear affirmative action". Employers must provide clear privacy notices before or at consent collection. Consent can be withdrawn easily, requiring the Data Fiduciary to cease processing within a "reasonable time". The Act introduces Consent Managers to streamline consent management.[13]

"Certain Legitimate Uses" in Employment -

A significant provision allows processing without explicit consent for "certain legitimate uses". This includes processing for employment purposes, safeguarding the employer from loss/liability (e.g., corporate espionage, trade secrets), or providing employee services/benefits. This implies a "deemed consent" for core employment functions, offering flexibility compared to GDPR. However, employers must transparently explain "legitimate use" and ensure proportionality, as general surveillance disclosures may be insufficient.[14]

C. RIGHTS OF DATA PRINCIPALS (EMPLOYEES)

Employees, as Data Principals, have defined rights:

- Right to Access: Request summary of personal data, purpose, and access recipients.
- Right to Correction: Request correction of inaccurate/incomplete data.
- Right to Erasure: Request deletion when data is no longer necessary or upon consent withdrawal, unless legally mandated.

---

[12] Data Protection Board of India: Role and Powers, INDIA LEGAL (Sept. 2, 2023), https://www.indialegal.com/legal-news/data-protection-board-of-india-role-and-powers/.

[13] GDPR and HR: Data Retention Periods, HR NEWS (last visited July 18, 2025), https://www.hrnews.co.uk/gdpr-and-hr-data-retention-periods/.

[14] Enforcement and Penalties under DPDP Act, 2023, INDIA LEGAL (Sept. 2, 2023), https://www.indialegal.com/legal-news/enforcement-and-penalties-under-dpdp-act-2023/.

- Right to Grievance Redressal: Raise concerns and seek timely resolution from the employer or DPO.[15]
- Right to Nominate: Appoint a person to exercise rights upon death or incapacity.
- Right to Withdraw Consent: Where applicable, withdraw consent at any time.

Data Principals also have duties, with penalties for false complaints or impersonation.

D. OBLIGATIONS OF DATA FIDUCIARIES (EMPLOYERS)

Employers face significant compliance burdens:

- Data Accuracy, Completeness, and Consistency: Ensure employee data is accurate, complete, and consistently maintained.
- Security Measures: Implement technical and organizational measures to protect data against unauthorized access, loss, or damage (e.g., encryption, RBAC, MFA, penetration testing). A Security Incident Response Plan (SIRP) is advised.
- Data Retention and Deletion: Erase data when consent is withdrawn or purpose is served, unless legally required. Draft rules specify retention periods and require 48-hour notice before deletion.[16]
- Notice Requirements and Enhanced Consent Mechanisms: Provide clear, distinct privacy notices and obtain consent via affirmative action.
- Data Protection Officer (DPO) for SDFs: SDFs must appoint an India-based DPO with privacy expertise, reporting to the board/CEO.
- Data Protection Impact Assessments (DPIAs) and Audits: SDFs must conduct DPIAs for high-risk processing and annual audits.
- Data Breach Notification Protocols: Notify the Data Protection Board and affected Data Principals of breaches that may cause harm.
- Vendor and Processor Management: Employers are accountable for Data Processors; mandatory contracts (DPAs) are crucial.
- Training and Awareness: Regular internal training for employees, especially HR, on data protection practices.

---

[15] DPDP Act 2023: Penalties for Non-Compliance, DATA INSIGHTS (Sept. 20, 2023), https://datainsights.co/dpdp-act-2023-penalties-for-non-compliance/.

[16] DPDP Act 2023: Understanding Data Principal Rights, DATA SECURITY COUNCIL OF INDIA (last visited July 18, 2025), https://www.dsci.in/content/dpdp-act-2023-understanding-data-principal-rights/.

- Cross-Border Data Transfers: Permitted to affiliates outside India, subject to future Central Government restrictions.[17]

E. ENFORCEMENT AND PENALTIES

The Data Protection Board of India (DPB) enforces the Act, handling disputes and grievances digitally. The DPB has civil court powers to inquire into breaches and impose penalties. Non-compliance incurs significant financial penalties, ranging from ₹50 Crore to ₹250 Crore per violation, with higher fines for security, breach notification, and children's data violations.

IV. GLOBAL PRIVACY NORMS: GDPR AND CCPA/CPRA IN THE EMPLOYMENT CONTEXT

A. GENERAL DATA PROTECTION REGULATION (GDPR)

GDPR applies to organizations processing personal data of EU individuals.[18]

Lawful Basis for Processing Employee Data:

GDPR requires one of six legal bases. Due to power imbalance, consent is often problematic in employment. Employers often rely on:[19]

- Contractual Necessity: For payroll or benefits.
- Compliance with Legal Obligations: For tax reporting or mandated records.
- Legitimate Interests: For fraud prevention or performance management, balanced against data subject rights.

Data Subject Rights:

GDPR grants comprehensive rights to employees:

---

[17] DPDP Act 2023: Data Retention and Deletion Obligations, DATA INSIGHTS (Sept. 20, 2023), https://datainsights.co/dpdp-act-2023-data-retention-and-deletion-obligations/.

[18] GDPR and Candidate Data: Best Practices for Recruitment, WORKABLE (last visited July 18, 2025), https://resources.workable.com/tutorial/gdpr-candidate-data-best-practices.

[19] General Data Protection Regulation, Regulation (EU) 2016/679, art. 6, 2016 O.J. (L 119) 1.

Right to be Informed, Access, Rectification, Erasure (Right to be Forgotten), Restriction of Processing, Data Portability, Object, and not to be Subject to Automated Decision-Making. Employers must respond within one month.

Employer Obligations:

Key obligations include:

- Data Protection Officer (DPO) Appointment: Mandatory for large-scale monitoring or sensitive data processing.
- Data Protection Impact Assessments (DPIAs): Mandatory for high-risk processing (e.g., systematic monitoring).
- Data Security Measures: Appropriate technical and organizational measures.
- Data Retention Policies: Data kept no longer than necessary; clear policies required.
- Cross-Border Data Transfers: Permitted only with adequate protection (e.g., Adequacy Decisions, SCCs, BCRs, explicit consent).

Enforcement and Penalties:

Violations can result in fines up to €20 million or 4% of global annual turnover, whichever is greater.

B. CALIFORNIA CONSUMER PRIVACY ACT (CCPA) AS AMENDED BY CPRA[20]

The CPRA, effective January 1, 2023, and enforceable from July 1, 2023, eliminated employee and B2B exemptions, extending consumer privacy rights to California employees, job applicants, and contractors. It applies to businesses meeting revenue or data processing thresholds.

Definition of Employee Data and Sensitive Personal Information:

"Personal information" is broadly defined to include identifiers and employment data. CPRA introduced "Sensitive Personal Information" (SPI), including social security numbers,

[20] Rights of the data subject, ICO (Information Commissioner's Office) (last visited July 18, 2025), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/.

financial credentials, precise geolocation, racial/ethnic origin, and health information, subject to additional protections.

Employee Rights:[21]

California employees have significant rights:

- Right to Know, Delete, Correct, Opt-Out of Sale or Sharing, Limit Use and Disclosure of Sensitive Personal Information, and Non-Discrimination. Employers must respond to requests within 45 days.

Employer Obligations:[22]

Employers subject to CCPA/CPRA have responsibilities including:

- Expanded Privacy Notices: Inform employees about data collection and use at or before collection.
- Data Inventory and Mapping: Understand what data is held, where, how processed, and shared.
- Identity Verification for DSRs: Verify requester identity.
- Data Minimization: Limit collection to what is "reasonably necessary and proportionate".
- Reasonable and Appropriate Security Measures: Security appropriate for data sensitivity.
- Data Retention Limitations: Data not retained longer than reasonably necessary; establish maximum retention periods.[23]

[21] GDPR and Candidate Data: Best Practices for Recruitment, WORKABLE (last visited July 18, 2025), https://resources.workable.com/tutorial/gdpr-candidate-data-best-practices.

[22] CPRA Employee Data: What Employers Need to Know, JACKSON LEWIS P.C. (Jan. 1, 2023), https://www.jacksonlewis.com/publication/cpra-employee-data-what-employers-need-know.

[23] Data Mapping and Inventory: A Key to Compliance, TRUSTARC (last visited July 18, 2025), https://www.trustarc.com/blog/data-mapping-and-inventory-a-key-to-compliance/.

Enforcement and Penalties:

Enforced by the California Privacy Protection Agency (CPPA) and Attorney General. Penalties: $7,500 for intentional, $2,500 for unintentional violations. Private right of action for data breaches due to inadequate security.[24]

V. HR PRACTICES IN TRANSITION: CHALLENGES AND OPPORTUNITIES

A. IMPACT ON KEY HR FUNCTIONS

Recruitment and Onboarding:

Extensive candidate data collection requires explicit consent for sensitive data and clear privacy policies. Data minimization is key; only job-related info should be collected. Storing "hot candidate" lists without consent is generally not allowed. DPDP Act and CCPA/CPRA extend these requirements to job applicants.

Performance Management and Payroll:

These functions involve highly sensitive data. Data accuracy and security are paramount, especially as data is used for decision-making or disclosed to benefits providers. Data retention periods are critical; data should not be retained longer than necessary. Clear data retention policies and secure deletion/anonymization are essential.

Employee Monitoring:

Balancing legitimate business interests (e.g., security, efficiency) with privacy rights is complex. Compliant monitoring requires:

- Transparency: Inform employees about monitoring, purpose, and data use.
- Lawful Basis: Legitimate interests (GDPR), legal obligation, contractual necessity, or DPDP Act's "legitimate use".
- Data Minimization & Proportionality: Collect only necessary data, avoid excessive surveillance.

[24] Data Protection Officer (DPO) under GDPR, GDPR.EU (last visited July 18, 2025), https://gdpr.eu/data-protection-officer/.

- DPIAs: Often mandatory for high-risk monitoring. US laws like ECPA and NLRA restrict monitoring. California law prohibits monitoring without knowledge/consent, recording conversations without mutual consent, or monitoring private areas. CPRA grants employees rights to know about monitoring data, request deletion, and limit sensitive data use .

B. DIGITAL TRANSFORMATION, CLOUD COMPUTING, AND AI[25]

Data Security and Privacy Challenges in Cloud Computing:[26]

Cloud computing introduces risks: data confidentiality, loss/theft, geographical storage issues, multi-tenancy security, and transparency issues from providers. Mitigation requires strong cybersecurity, robust identity access management, and due diligence for cloud service providers.

Ethical and Privacy Implications of AI in HR:[27]

AI in HR (e.g., resume screening, performance automation) raises concerns:

- Bias: AI can perpetuate discrimination from biased training data].
- Lack of Transparency (Black Box Problem): Difficulty understanding AI decisions hinders accountability
- Unintended Consequences: Over-reliance on AI can lead to flawed, impersonal decisions.
- Privacy Risks: AI can analyze vast personal data, leading to over-collection or unauthorized use

[25] AI in HR: Benefits, Risks, and Ethical Considerations, FORBES (last visited July 18, 2025), https://www.forbes.com/sites/forbestechcouncil/2023/07/20/ai-in-hr-benefits-risks-and-ethical-considerations/.
[26] Cloud Computing Security and Privacy Challenges, RESEARCHGATE (last visited July 18, 2025), https://www.researchgate.net/publication/320000000_Cloud_Computing_Security_and_Privacy_Challenges.

[27] The Impact of AI on HR: Ethical and Legal Considerations, SHRM (last visited July 18, 2025), https://www.shrm.org/resources-and-tools/hr-topics/technology/pages/the-impact-of-ai-on-hr-ethical-and-legal-considerations.aspx.

Mitigation Strategies for AI in HR:

- Diverse Training Data & Bias Audits: Use representative data and conduct regular bias audits.
- Human Oversight: Ensure human review in AI-driven decisions.
- Transparency and Explainable AI (XAI): Be transparent about AI use; develop XAI for understanding rationale.
- Data Minimization and Purpose Limitation: Collect only necessary data.
- Explicit Consent: Obtain informed consent for data use in AI systems.
- Robust Cybersecurity Measures: Protect personal data from breaches.
- Privacy by Design: Embed privacy safeguards from early design stages.
- Data Anonymization/De-identification: Obfuscate PII while preserving data utility.
- Ethical AI Development: Adopt ethical principles (fairness, accountability, transparency)
- Continuous Monitoring and Auditing: Regularly audit AI systems for compliance.

C. STRATEGIC COMPLIANCE AND RISK MITIGATION:[28]

- Data Mapping and Inventory: Understand data collection, processing, storage, and flow to identify risks and ensure compliance.
- Policy Development and Updates: Develop and maintain clear, up-to-date data policies aligned with regulations (data retention, access controls, privacy notices).
- Employee Training and Awareness: Regular training for all employees, especially HR, on data protection practices.
- Vendor Due Diligence and Contractual Agreements: Thorough due diligence on third-party vendors and mandatory Data Processing Agreements (DPAs)
- Privacy by Design and Default: Embed privacy into system design from the outset
- Incident Response Planning: Comprehensive plan for data breaches, including detection, response, mitigation, and notification within mandated timeframes.[29]

[28] Ethical Implications of AI in HR: A Comprehensive Guide, AI IN HR (last visited July 18, 2025), https://aiinhr.com/ethical-implications-of-ai-in-hr/.
[29] Bias in AI: Types, Causes, and Mitigation Strategies, IBM (last visited July 18, 2025), https://www.ibm.com/topics/bias-

VI. CASE STUDIES: REAL-WORLD IMPLICATIONS OF DATA PRIVACY LAWS IN HR

Examining specific case studies provides practical insights into the challenges and consequences of managing employee data under evolving privacy regulations. These examples highlight the significant impact of non-compliance and the importance of proactive data governance.

A. GDPR ENFORCEMENT: BRITISH AIRWAYS AND MARRIOTT DATA BREACHES

The GDPR has demonstrated its enforcement power through substantial fines for data breaches, even when they originate from third-party vulnerabilities. While these cases were not exclusively focused on employee data, they illustrate the broad scope of personal data covered and the severe penalties for inadequate security measures that could easily extend to internal HR systems.

- British Airways (2019): The UK's Information Commissioner's Office (ICO) initially intended to fine British Airways £183.39 million (later reduced to £20 million) for data breach affecting approximately 400,000 customers and employees. The breach, which occurred in 2018, involved attackers diverting user traffic from the airline's website to a fraudulent site, harvesting personal and financial details. The ICO found that BA had inadequate security measures in place to protect its systems, leading to the breach. This case underscored the principle of accountability under GDPR, holding organizations responsible for protecting personal data, regardless of how the breach occurred, and highlighted the need for robust cybersecurity across all data touchpoints, including those that might hold employee information. The fine, though reduced, was still one of the largest under GDPR at the time, signaling a strong deterrent message.
- Marriott International (2020): Marriott faced a proposed fine of £99.2 million (later reduced to £18.4 million) from the ICO following a cyberattack that exposed the personal data of approximately 339 million guests globally, including names, addresses, passport numbers, and payment card details. The breach originated from the systems of Starwood Hotels and Resorts, which Marriott acquired in 2016. The ICO's investigation found that Marriott failed to conduct sufficient due diligence

when acquiring Starwood and neglected to implement appropriate security measures to protect the acquired systems. This case emphasizes the importance of thorough data privacy and security due diligence during mergers and acquisitions, and the continuous obligation to protect all personal data, including that of employees if such systems were also compromised. It highlights that an organization inherits the data protection liabilities of acquired entities.

These cases, though primarily consumer-focused, serve as stark warnings for HR departments. They demonstrate that insufficient security, whether due to direct negligence or inadequate vendor/acquisition due diligence, can lead to massive fines. HR systems, containing highly sensitive employee data, are equally vulnerable and require the same, if not greater, level of protection and scrutiny.

B. CCPA/CPRA ENFORCEMENT: EMPLOYEE DATA IMPLICATIONS:

With the expiration of the employee exemption under CPRA, California employers now face direct enforcement actions related to employee data. While specific, large-scale public fines solely on employee data are still emerging due to the CPRA's recent full enforceability, general CCPA enforcement actions illustrate the types of violations that could apply to HR.

- Sephora (2022): The California Attorney General fined Sephora $1.2 million for failing to process consumer opt-out requests via a Global Privacy Control (GPC) signal and for failing to inform consumers that it was selling their personal information. While this case focused on consumer data, the principles of respecting opt-out rights and providing clear privacy notices are directly applicable to employee data under CPRA. If an HR system were to "sell" (broadly defined under CCPA/CPRA to include sharing for cross-context behavioral advertising) employee data without proper notice and an opt-out mechanism, it could face similar penalties. This emphasizes the need for HR to ensure that any data sharing with third-party vendors (e.g., for benefits, wellness programs) is clearly disclosed and that employees' rights to opt-out are honored.
- Hypothetical CPRA Employee Data Case: Consider an employer who uses an AI-powered tool for employee performance monitoring. If this tool collects excessive data beyond what is "reasonably necessary and proportionate" for performance evaluation, or if the employer fails to provide a clear privacy notice to employees

about the data collected, its purpose, and how employees can exercise their rights (e.g., right to know, right to delete, right to limit use of SPI), it could face significant fines under CPRA. Furthermore, if the monitoring tool collects "sensitive personal information" (e.g., precise geolocation, health data inferred from activity patterns) and the employer fails to provide the "Right to Limit Use and Disclosure of Sensitive Personal Information," this would be a direct violation. This hypothetical scenario highlights the direct applicability of CPRA's stringent requirements to HR's use of technology.

C. ETHICAL AND PRIVACY IMPLICATIONS: AI BIAS IN HR:

The use of AI in HR, while promising efficiency, has raised significant ethical and privacy concerns, particularly regarding bias.

- Amazon's AI Recruiting Tool (2018): Perhaps the most widely cited example is Amazon's experimental AI recruiting tool, which was reportedly scrapped because it showed bias against women. The AI was trained on a decade of resume submissions, most of which came from men, reflecting the male dominance in the tech industry. Consequently, the AI penalized resumes that included words like "women's" (e.g., "women's chess club captain") and downgraded candidates who graduated from all-women's colleges. This case starkly illustrates how AI, when trained on biased historical data, can perpetuate and even amplify existing societal inequalities, leading to discriminatory outcomes in recruitment. From a privacy perspective, the collection and processing of data that leads to such biased inferences, without transparency or a mechanism for redress, poses significant ethical and legal challenges. It underscores the need for rigorous bias audits, diverse training data, and human oversight in AI-driven HR processes.

D. DPDP ACT: POTENTIAL IMPLICATIONS FOR HR (ILLUSTRATIVE SCENARIO):

Given the DPDP Act's recent enactment, public enforcement cases are yet to emerge. However, based on its provisions, illustrative scenarios can highlight potential impacts on HR.

- Scenario: Unjustified Employee Monitoring by an Indian Employer**:** An Indian company implements a new comprehensive employee monitoring system that tracks keystrokes, screenshots, and web browsing activity on company devices without providing a clear, specific, and detailed privacy notice to employees. While the DPDP Act allows for "legitimate use" in employment, general surveillance without clear purpose and proportionality would likely be challenged. If an employee's personal data (e.g., health information inadvertently captured in a screenshot, or personal communications) is collected and processed without explicit consent or a strong, demonstrable legitimate use, and without adequate security measures, the employer could face significant penalties from the Data Protection Board of India. Furthermore, if a data breach were to occur involving this excessively collected and inadequately protected monitoring data, the penalties could be substantial, potentially reaching up to ₹250 Crore. This scenario emphasizes the need for transparency, proportionality, and robust security even under the "legitimate use" provision of the DPDP Act. These case studies and scenarios underscore that data privacy is not merely a theoretical legal concept but a practical challenge with significant financial, legal, and reputational consequences for organizations that fail to adapt their HR practices to the evolving regulatory landscape.

VII. CONCLUSION

The evolving landscape of employee data and privacy laws, driven by global regulatory convergence and digital advancements, fundamentally transforms HR practices. Foundational data protection principles are universally accepted, yet nuanced implementation and heightened protection for sensitive data necessitate careful localization. India's DPDP Act, 2023, is a significant stride, defining roles, extending applicability, and introducing "certain legitimate uses" for employment data. While offering flexibility, this provision demands transparent communication from employers. The Act empowers employees with robust rights and imposes extensive obligations on employers, with substantial penalties for non-compliance. Concurrently, GDPR sets high standards in Europe, emphasizing lawful bases beyond consent and comprehensive data subject rights. The CCPA/CPRA in the U.S. significantly expands privacy protections to California employees, requiring detailed notices and strict data retention. Digital transformation, cloud computing, and AI introduce efficiency but also complex challenges. Cloud environments pose security and privacy risks, while AI in

HR carries risks of bias and lack of transparency. Mitigation requires diverse training data, human oversight, explainable AI, data minimization, explicit consent, and privacy-by-design. Ultimately, HR's transition is a shift towards embedding data privacy as a core organizational value. Proactive data governance, comprehensive data mapping, clear policies, continuous training, rigorous vendor due diligence, and privacy by design are essential. Continuous vigilance and adaptation are crucial for HR to leverage data effectively while upholding privacy and fostering trust.