Journal of Science and Technology Excellence
ISSN: **3108-3102**| Volume 2 Issue 1 January-March 2026
www.jstejournal.com **DOI**: https://doi.org/10.65713/jstev2i141 **JSTE-41**

EMPLOYEE DATA PRIVACY AND HR ETHICS AT ACCENTURE

[#1]Dr B SANKAR NAIK, *Professor,*
[#2] GOONI NAGASREE, *MBA Student,*
Department of MBA,
VISWAM ENGINEERING COLLEGE (Autonomous), ANGALLU, MADANAPALLE, AP.

ABSTRACT: This investigation investigates Accenture's human resource (HR) ethics and employee data privacy. Accenture is a global provider of professional services that operates in a highly digital and data-driven environment. The protection of employee data has become more critical for businesses as they implement more advanced technologies, such as cloud-based HR solutions, artificial intelligence, and analytics. The abstract outlines Accenture's implementation of comprehensive governance structures, adherence to international data protection regulations such as GDPR, and the integration of ethical principles into HR procedures to safeguard the privacy of its employees' data. Consent, transparency, data reduction, privacy, and the responsible use of employee information are among the significant ethical issues that are addressed. The paper also underscores Accenture's dedication to the management of confidential employee data in a variety of cultural and geographic contexts, as well as the establishment of trust and the exercise of responsibility. Accenture ensures that HR ethics are in compliance with data privacy requirements, thereby enhancing employee trust, organizational integrity, and long-term business practices. This also mitigates the likelihood of legal action and brand damage. The results indicate that ethical HR data management is necessary to preserve a secure, transparent, and equitable workplace in the digital age.

Keywords: *Employee Data Privacy, HR Ethics, Data Protection Policies, Confidentiality Management, Ethical Data Handling*

I. INTRODUCTION

HR ethics and employee data privacy are to safeguard sensitive employee data (including health, performance, and demographics), while simultaneously promoting trust and complying with legal mandates (including the DPDP Act and GDPR). This is especially important in the context of HR analytics, as bias may be a concern. Some essential actions include undertaking regular audits, providing employee training, implementing secure technology (such as encryption and access controls), and establishing explicit guidelines. These measures are instrumental in protecting the rights of both individuals and enterprises.

The ethical considerations of HR analytics are essential for the responsible use of data and the protection of employee privacy. This involves prioritizing ethics, being transparent, and adhering to the law when making decisions.

The treatment of employees by businesses has been altered as a consequence of human resources (HR) analytics. Businesses can improve their hiring, performance management, and employee engagement decisions by leveraging data-driven insights. Nevertheless, the

Journal of Science & Technology Excellence
Journal of Science and Technology Excellence
ISSN: **3108-3102**| Volume 2 Issue 1 January-March 2026
www.jstejournal.com **DOI**: https://doi.org/10.65713/jstev2i141 **JSTE-41**

proliferation of HR analytics has resulted in substantial ethical concerns, particularly in the context of protecting employee privacy. In the current digital era, it is imperative that businesses guarantee the security of personal information and comply with ethical standards when collecting and analyzing substantial quantities of employee data. Ethical considerations in HR analytics are essential to guarantee that data is managed appropriately and employees' privacy is safeguarded in compliance with the law.

In this era of rapid technological advancement, human resources (HR) analytics has become increasingly significant as an instrument to aid HR departments in making decisions. Nevertheless, it is imperative to evaluate the ethical and privacy implications of this powerful tool as companies increasingly rely on data-driven insights. Particularly in the context of safeguarding against external intrusions, it is imperative to guarantee the security and privacy of your employees' personal information.

Nevertheless, an employer's access to employee information is limited by the necessity to protect data and privacy laws. The majority of privacy regulations permit the collection of information that is genuinely essential. The majority of the time, employees must be informed about the use of their data and provided with the opportunity to make corrections. Retention policies, which dictate the duration of data retention prior to destruction, may also be necessary, particularly for the data of departing personnel.

When employing foreign nationals, it is imperative to comply with both international and US regulations. For instance, the GDPR mandates that US organizations that employ personnel in France or Germany comply with its regulations.

As digital environments continue to develop, businesses must strike a balance between safeguarding employee privacy and ensuring the security of their operations. The data management practices of experts in privacy, compliance, and security are being scrutinized increasingly due to the increasing stringency of international regulations and the desire for greater transparency among employees. Companies are obligated to maintain privacy regulations while simultaneously cultivating trust. They must achieve an equilibrium between the necessity of monitoring and ethical data protection.

II. STEPS TO PROTECTING YOUR EMPLOYEE DATA

It is logical that protecting employee data can be a difficult task. The measures outlined below can be taken to safeguard the data of your employees.

Know the law

It is imperative to comprehend one's obligations regarding data management in order to formulate a protection strategy. Ensure that you are cognizant of the federal, state, and local regulations that pertain to your business, as conducting business in other states and countries may present a challenge.

Establish data privacy policies and security measures

Comprehend the item you are collecting, the location where it is being stored, and the source from which it is being collected. Establish regulations that incorporate your data protection strategy and implement specific security measures.

Journal of Science & Technology Excellence
Journal of Science and Technology Excellence
ISSN: **3108-3102**| Volume 2 Issue 1 January-March 2026
www.jstejournal.com **DOI**: https://doi.org/10.65713/jstev2i141 **JSTE-41**

Limit employee access to data: Adhere to the "principle of least privilege" and provide staff with access to only the data that is essential for them to perform their responsibilities.

Secure physical devices: Hard passwords or biometric access should be required for company laptops and phones, and remote erasure should be feasible.

Encrypt data: When transmitting data, implement encryption on servers and devices.

It is imperative that you are forthright with your employees regarding the security of your data. Being aware of the data you are collecting and the methods you are using to safeguard it will facilitate the development of trust over time.

Limit access only to necessary parties

Employees who require access to private information, such as HR personnel, should have it. Implement strategies such as multi-factor authentication and conduct routine assessments of your security protocols.

Screen employees with access to sensitive data

Ensure that an employee has successfully completed a background check prior to granting them access to critical company information. Obtain their signature on a contract that delineates their obligations and the consequences for violating the regulations. Ensure that all individuals who have access are regularly verified and that the credentials of those who have either left the company or are no longer needed are removed.

Provide training to employees

Criminals are perpetually devising novel strategies. They have the ability to directly target your staff by deceiving them into clicking on a link in an email (phishing) or providing them with information over the phone, in addition to successfully breaching into your network. Regular training for all employees, not just those who manage sensitive information, can enhance data security.

Have a plan in place

Hacking is a reality. In the event that they do, you must be adequately equipped. It is imperative that your organization establishes a plan to manage the consequences. It should be updated on a regular basis, as is the case with all security training. Furthermore, it is imperative to engage in discussions regarding the strategy with all of the organization's most critical personnel.

Choose the right software

The appropriate software can be used to protect sensitive data and employee devices. It is imperative to acquire the appropriate software for your organization. It can assist in maintaining the security of your organization, regulating access, and guaranteeing compliance with industry regulations.

III. REVIEW OF LITERATURE

Idowu, E. (2025). The primary focus of this qualitative study is the techniques of gathering, storing, monitoring, and safeguarding employee data. It investigates moral dilemmas associated with the utilization of human resources information systems (HRIS). It underscores concerns such as unauthorized access, excessive employee surveillance, and unethical use of HR data. The study underscores the importance of rigorous ethical

ISSN: **3108-3102**| Volume 2 Issue 1 January-March 2026
www.jstejournal.com **DOI**: https://doi.org/10.65713/jstev2i141 **JSTE-41**

frameworks, open governance, encryption restrictions, and anonymization techniques in order to safeguard sensitive data. This is the result of policy analysis and consultations with HR specialists. It also addresses the repercussions of unethical conduct, including the loss of credibility, the consequences of being unjust, and the possibility of legal action.

Mehra, G. (2025). This essay investigates the impact of international privacy laws, including the GDPR, CPRA, and India's DPDP Act (2023), on HR practices. It contends that the digital transformation in HR necessitates the transition to privacy-by-design and rigorous data control. Various legal systems are examined in a comprehensive research that investigates recruiting, performance management, and employee monitoring. Mehra addresses the potential hazards of cloud computing and AI, such as a lack of transparency, prejudice, and challenging compliance.

Zhong, C., & Feng, N. (2025). Using panel data from Chinese businesses (2011–2023), this empirical study investigates the impact of firm privacy protection on the labor share of income, a metric of employee well-being. The results indicate that workplaces with robust privacy policies are more equitable, as enhanced privacy governance is associated with a higher proportion of labor income. This effect is primarily mediated by the distribution of highly trained human resources and strong consumer relationships, as per mechanism research.

Shrivastav, P., Tiwari, D., & Lakshmi, G. (2024). This paper investigates the ethical, legal, and practical implications of employee privacy in contemporary workplaces that incorporate artificial intelligence, data analytics, and digital surveillance. It exhibits the rapid adoption of technology in contrast to the slow pace at which laws are maintaining pace, and it emphasizes the deficiencies in current privacy regulations. The research contends that open communication, informed consent, and ethical supervision are indispensable for the purpose of alleviating employee privacy concerns and reestablishing trust. It analyzes case studies and legal systems from around the globe to suggest equitable privacy policies.

Ebert, I. (2024). This study examines the ethical implications of the growing utilization of big data analytics in HRM systems. It illustrates the potential consequences of collecting an abundance of employee data, including the violation of privacy regulations, the misuse of data, and the implementation of unjust decisions. According to the author, big data has the potential to enhance the effectiveness and future-orientedness of HR; however, it also raises ethical concerns regarding transparency, impartiality, and the acquisition of employee consent. The investigation examines the potential for algorithmic decision-making to unintentionally reinforce prejudice, restrict employee autonomy, and diminish accountability if it is not rigorously regulated. Ebert emphasizes the importance of establishing ethical guidelines, well-organized risk assessments, and comprehensive governance structures to prevent employees from exploiting their data.

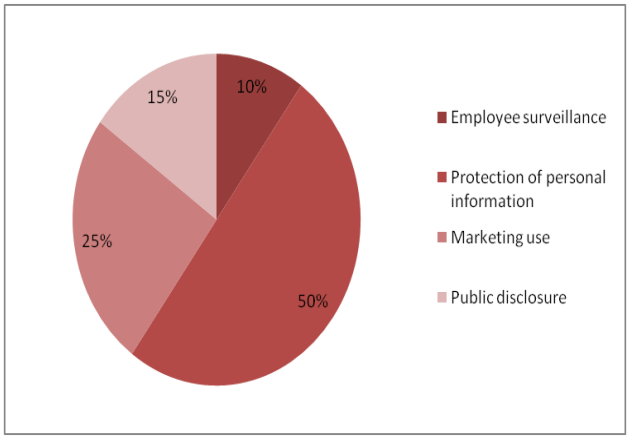
Álvarez-Gutiérrez, F. J. (2023). The current academic literature on human resources analytics is the subject of this systematic review, which places a particular emphasis on the ethical concerns associated with the use of employee data. Informed consent, transparency, trust in organizations, and data privacy are all persistent issues, according to the report. It illustrates the extent to which workers' autonomy and sense of justice can be diminished by

Journal of Science and Technology Excellence
ISSN: **3108-3102**| Volume 2 Issue 1 January-March 2026
www.jstejournal.com **DOI**: https://doi.org/10.65713/jstev2i141 **JSTE-41**

inadequate HR analytics management. The author provides conceptual frameworks to bolster the development of HR analytics techniques that are both morally sound and long-lasting. These frameworks underscore the importance of transparency in data management, soliciting feedback from interested parties, and adhering to the law. The evaluation also emphasizes the importance of ensuring that analytical processes comply with ethical HR norms to prevent individuals from exploiting data-driven insights.

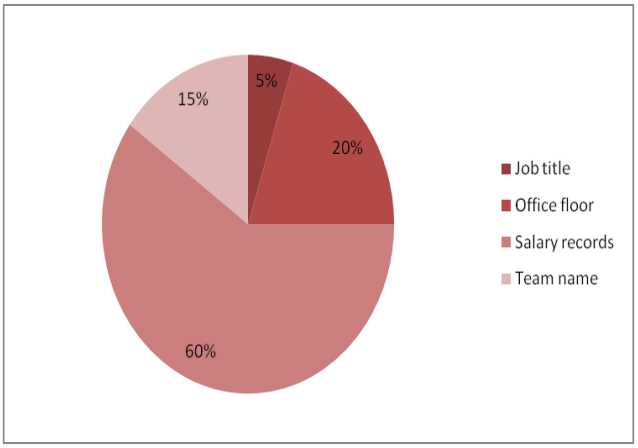
IV. PERFORMANCE EVALUATION

1. What is Accenture's primary objective with respect to safeguarding employee data?



As per the investigation, the primary concern of 50% of respondents was the manner in which marketing exploits employee data. This suggests that individuals are extremely apprehensive about the use of their personal data for purposes other than human resources. Data security and privacy are of paramount importance to employees, as evidenced by the fact that personal information protection is ranked second at 25%. In comparison to other challenges, employee surveillance (10%) and public exposure (15%) are perceived as less frequent or simpler to manage within the organization.

2. Which employee data is treated as confidential at Accenture?

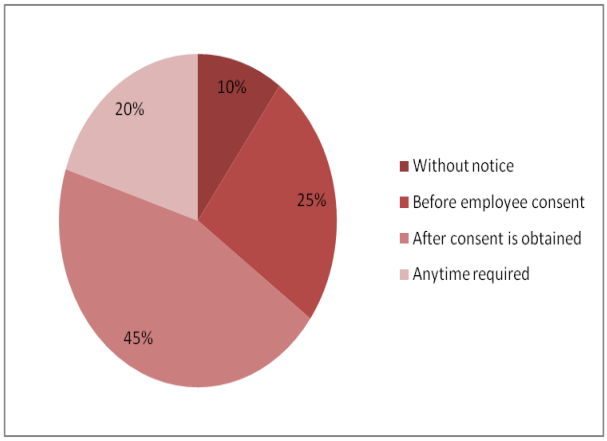


According to the results, wage records were the most sensitive form of employee data, as 60% of respondents expressed concern. Twenty percent of the information pertains to the workplace floor, suggesting that individuals are somewhat cognizant of privacy concerns associated with their physical location. Job titles (5%) and team names (15%) are perceived

Journal of Science & Technology Excellence
Journal of Science and Technology Excellence
ISSN: **3108-3102**| Volume 2 Issue 1 January-March 2026
www.jstejournal.com **DOI**: https://doi.org/10.65713/jstev2i141 **JSTE-41**

as less sensitive by individuals, which is why it is permissible to discuss them in the workplace.

3. When does Accenture acquire personal data regarding its employees?



The majority of respondents (45%) are of the opinion that data access should only be granted with the employee's consent. This illustrates the importance of authorization in the context of data privacy. It is possible that there are ethical breaches, as a substantial portion of the population (25%) believes that access should be prioritized over consent. Ten percent of requests are made without prior notice, while twenty percent are made at any time. This illustrates the importance of morality and integrity to individuals.

V. CONCLUSION

The employee data privacy and human resource (HR) ethics of Accenture are examined in this study. Accenture is a global provider of professional services operating in a highly digital and data-driven environment. It has become increasingly crucial for firms to safeguard employee data as they adopt more sophisticated technologies like analytics, artificial intelligence, and cloud-based HR solutions.

The abstract describes how Accenture uses robust governance structures, complies with international data protection regulations like GDPR, and ensures that ethical principles are included into HR procedures to preserve the privacy of its employees' data. Important ethical topics covered include consent, transparency, data reduction, privacy, and responsible use of employee information.

The paper also emphasizes Accenture's commitment to making moral decisions, building trust, and exercising responsibility while managing sensitive employee data in a range of cultural and geographic contexts. Accenture increases employee trust, organizational integrity, and long-term business practices by ensuring that HR ethics are compliant with data privacy requirements. This also reduces the possibility of legal action and brand damage. The findings demonstrate that maintaining a fair, transparent, and secure workplace in the digital era requires ethical HR data management.

Journal of Science and Technology Excellence
ISSN: **3108-3102**| Volume 2 Issue 1 January-March 2026
www.jstejournal.com **DOI**: https://doi.org/10.65713/jstev2i141 **JSTE-41**

REFERENCES

1. Duska, Ronald. "Employee Rights." In Issues in Business Ethics. Springer International Publishing, 2022.
2. Moriarty, Jeffrey. "Employee ethics and rights." In The Routledge Companion to Business Ethics. Routledge, 2018.
3. Estlund, Cynthia. "Individual employee rights at work." In Comparative Employment Relations in the Global Economy. Routledge, 2020.
4. Custers, Bart, Alan M. Sears, Francien Dechesne, Ilina Georgieva, Tommaso Tani, and Simone van der Hof. EU Personal Data Protection in Policy and Practice. T.M.C. Asser Press, 2019.
5. Munir, Abu Bakar. Personal data protection in Malaysia: Law and practice. Sweet & Maxwell Asia, 2010.
6. Lefkowitz, Joel, and Rodney L. Lowman. "Ethics of Employee Selection." In Handbook of Employee Selection. Routledge, 2017.
7. Moriarty, Jeffrey. "Employee ethics and rights." In The Routledge Companion to Business Ethics. Routledge, 2018.