Data Privacy in Public Employment: Impacts of the UK GDPR and Nigeria's NDPR 2023

Abubakar Solihu Orisankoko

Public Administration, Highstone International University, USA

DOI: https://doi.org/10.47772/IJRISS.2026.100500202

Received: 07 March 2026; Accepted: 12 March 2026; Published: 26 May 2026

ABSTRACT

This study examines the effect of the United Kingdom's General Data Protection Regulation (UK GDPR) and Nigeria's Data Protection Act (NDPA) 2023 in influencing human resource management (HRM) operations within public sector organisations. A mixed-methods research approach, which combined questionnaire surveys with document reviews to study essential HR operations that include recruitment and personnel records management, employee monitoring, health data administration, and termination procedures, has been adopted. The research shows that UK HR practices experienced major changes because of GDPR, through its enforcement of compliance requirements, employee rights protection, and institutional accountability measures. On the other hand, the NDPA 2023 was legislated recently by the Nigerian government to engender a modern legal structure within the scheme of development, yet public sector implementation faces obstacles because of several inhibiting factors like insufficient public knowledge, restricted financial backing, weak regulatory supervision and compliance enforcement. The NDPR 2023 is a total replacement for the erstwhile Nigeria Data Protection Regulation (NDPR) 2019, which was in operation until its repeal in June 2023. The research demonstrates that institutional theory shows legislative frameworks that enforce rules do not ensure compliance because institutional power, together with staff knowledge and professional codes, determines the outcome. The research study advances existing knowledge about international data protection practices while delivering practical guidance to HR professionals, governmental bodies, and employees who operate in both domestic and foreign settings.

Keywords: Data protection, UK GDPR, NDPA 2023, human resource management, public sector, institutional theory, employee privacy, compliance

INTRODUCTION

Personal data is one of the most important human property that organisations feed on in the digital age. HRM departments in the workplace, especially in the public sector, handle a lot of personal employee information, like during hiring process, payroll information, medical records, performance appraisals, and records of discipline. Governments in many jurisdictions of the world have put in place strict rules about data protection to control how data is collected, processed, stored, and shared. This is because people are worried about digital privacy, cyber threats, and data abuse (Sharma and Kumar, 2023). The term Public service is interpreted to encompass the subset of civil service. The two names are sometimes used interchangeably; nonetheless, there exists a subtle distinction that delineates their respective scopes. Public service is considered a component of government entities, statutory businesses, and public institutions that directly engage with the public. The interface manifests in different manners, often categorized as either a business enterprise or a service enterprise. The latter addresses the public as a platform primarily designed to provide mandatory social services that the government is obligated to deliver to its citizens (Kings, 2023).

The efforts of government agents in this servicer are not compensated directly by the beneficiaries. This includes the military, police, public schools, utilities, state-owned businesses, social workers, government lawyers, firefighters, and other such groups. The first one is the part of the public service that makes money. There are enterprises that make the government huge revenue like hospitals, tourism, tax agents, and more. This classification is contingent upon the governmental system present in each jurisdiction (Sharma and Kumar,

2023). Not all public institutions categorized under income generation may be defined as such, as some, in nations like the United Kingdom, function without producing revenue for the government. The National Health Service (NHS), established in 1948 as the public healthcare system, does not generate revenue for the government in the strict sense of a public enterprise, in contrast to the Federal Government owned Hospitals in Nigeria.

The advent of the UK GDPR and NDPR 2023 (Nigeria) underscores the need for all individuals to protect the citizens of the nation, while the NDPR additionally mandates foreigners to ensure the protection of the personal data of Nigerians living in or visiting foreign territories, according to *Section 2(1)* NDPA 2023. While the NDPA restricts its scope of processing personal data, its focus is surprisingly just on "Personal Data" without determining the data subject within the Nigerian territory. Article 3(2) UKGDPR clearly states that the law protects the data subject within the United Kingdom, regardless of where the controller and processor domiciles. It is therefore not clear whether or not the Act is made to protect Nigerians or non-Nigerians. There is equally no mention of natural person living in Nigeria in the NDPA 2023. Although, *Section 9(2)(a)* NDPR 2023 mentioned a Nigerian but only in connection with the appointment of the council members. Equally, another key word/phrase in the data protection regulatory regime is "Natural Person". This is only mentioned under *Section 65* of the NDPA 2023 in connection with "*pseudonymisation" and under Section 65(a) – "sensitive personal data"*. None of these key words and/or phrase has been mentioned directly and indirectly in connection with the subject of protection of this Act. It lives one to wonder to wonder is the NDPA 2023 has been enacted to preserve, secure and protection the core value of the Nigerian populace. The UK case of *S. and Marper v. United Kingdom* (No. 30562/04, 30566/04) [2008] ECHR 1581 and the EUHR case law of *Catt v. United Kingdom* (Application No. 43514/15) have given proper delineating interpretation of the "data subject" of data protection law.

It might be contended that *Article 1(2)-(3) of the General Application and Implementation Directive (GAID) 2025* applies, by arguing that by virtue of that provision, the data subject or natural person who the NDPA 2023 seeks to protect has been clarified. Such an argument would be flawed given that before there could be a directory or explanatory note, the substantive law must have been enacted. In *Dangana vs. Usman (2013) 6 NWLR (PT. 1349) 50*, Court reiterated that where statutory words are clear, no extraneous aids (like directives or memoranda) can be invoked to supply omissions. It was established as a principle through the case of *A.-G. Federation vs. A.-G. Abia & Ors (No. 2) (2002) 6 NWLR (Pt. 764) 542* that Where a statutory provision is silent, courts cannot rely on an explanatory note to supply the omission. In that case, the Supreme Court held that explanatory memoranda cannot be used to add to or subtract from the words of a statute**.** Their role is interpretative, to clarify ambiguity., See also *Chief Obafemi Awolowo vs. Alhaji Shehu Shagari & 2 Others (SC.62/1979) (1979) All N.L.R. 105*. This position has been substantiated in *R (Public Law Project) v Lord Chancellor* [2016] UKSC 39, where the court held that Secondary legislation (statutory instruments) cannot be used to make provisions inconsistent with or to fill substantive gaps in the enabling Act. It was also clarified in *R v Secretary of State for the Environment, ex p. Spath Holme Ltd* [2001] 2 AC 349 (HL) that that explanatory notes cannot alter the meaning of statutory provisions; they can only be used as an aid to interpretation if there is genuine ambiguity.

This is not the case with the former Regulation (Nigeria Data Protection Regulation 2019). *Regulation 1.2 (b) and (c)* NDPR 2019 expressly stated that the Regulation is meant to protect Nigerians at home and in the diaspora, regardless of where the personal data is being processed. See the case of *The Incorporated Trustees of Paradigm Initiative for Information Technology Development & Ors vs the Attorney General of the Federation & Ors (CA/L/556/2017) and; Incorporated Trustees of Digital Rights Lawyers Initiative & ORS vs NIMC (2021) LPELR-55623(CA).*

The UK GDPR started its operations in January 2021 when the United Kingdom exited the European Union. The UK version of the EU GDPR kept the essential elements but implemented various modifications to these provisions (Sharma and Kumar, 2023). The law requires public sector organisations to protect employee (data subject) rights and disclose their practices and safeguard personal data through their combination with the Data Protection Act (DPA) 2018. Organisations face major financial penalties and damage to their reputation and public trust when they fail to follow the established rules. The Nigeria Data Protection Regulation (NDPR) 2019 was Nigeria's first attempt at protecting data and was a secondary law.

However, it was limited in terms of how far it could be enforced. The Nigeria Data Protection Act (NDPA) 2023 received approval to create stronger legal protections (Babalola, 2022). The Act grants additional rights to data subjects while creating the Nigeria Data Protection Commission (NDPC) as the main regulatory body and setting clear guidelines for public and private sector organisations.

Due to the fact that HR staff are in charge of employee data, these laws have a direct effect on how HR departments work. Organisations need to implement, administrative and technical solutions together with structural modifications, which include staff education, Data Protection Officer recruitment, and Data Protection Impact Assessment completion cum HR policy updates based on legal processing requirements. The evaluation of Nigeria's NDPA 2023 alongside the UK's GDPR becomes essential because these regulations will affect public sector HRM operations in two main ways:

(1) The comparison shows what Nigeria can learn from the UK's more advanced system, and

(2) The analysis reveals the specific difficulties which each nation encounters in protecting employee information.

Problem Statement

Public sector organisations face mounting challenges in managing employee data under evolving digital privacy regimes. HR departments handle sensitive records, including payroll, performance, health, and recruitment data, requiring robust protection to ensure legal compliance, ethical integrity, and employee trust. Despite the high standards of UK GDPR and Nigeria's Data Protection Act 2023 (NDPA), implementation remains problematic.

In the UK, post-Brexit GDPR enforcement exposes persistent difficulties, particularly in employee monitoring, data minimization, and delayed Subject Access Request responses, raising litigation and reputational risks (Babalola, 2022). Some of the cases include *Raine v JD Wetherspoon Plc* (2025) EWHC 1593 (KB), The Court ruled that an employer's oral disclosure of an employee's emergency contact number, obtained deceptively from her personnel file, constituted unlawful "processing" under the GDPR. It also affirmed that employees have a reasonable expectation of privacy over such information, upholding claims for misuse of private information and breach of confidence; *Bekoe v Islington LBC* (2023) EWHC 1668 (KB), where the court found the London Borough of Islington in breach of data protection law for its handling of Mr. Bekoe's Data Subject Access Request (DSAR). The authority's response was four years late, provided incomplete information, and involved the loss or destruction of legal files. The court ruled these actions breached Articles 5 (data protection principles), 12 (transparency), and 15 (right of access) of the UK GDPR, awarding Mr. Bekoe £6,000 in damages. Nigeria's NDPA, which replaced the NDPR 2019, signals progress toward modernization but is hindered by inadequate funding, weak institutional enforcement, limited HR training, and poor awareness of regulatory obligations (Sharma & Kumar, 2023).

The central issue lies in HR departments' limited capacity to meet statutory requirements, often due to insufficient technical expertise and misalignment between security and access systems. These deficits elevate risks of data breaches, non-compliance penalties, employee dissatisfaction, and public trust erosion. Evaluating the practical implications of UK GDPR and NDPA 2023 in term of impacts is therefore essential for understanding how institutional capacity, enforcement culture, and legal maturity shape compliance strategies in Nigeria and comparable contexts.

Research Gap

While substantial scholarship examines the EU GDPR's business implications, its influence on public sector HR is overlooked. In Nigeria, the pivotal NDPA 2023 has been enacted, yet research remains focused on its predecessor or the private sector, creating a significant knowledge gap. Similarly, comparative analysis of Nigerian and UK data protection systems is limited, despite their contrasting enforcement maturity. This study therefore bridges this gap through a systematic analysis of the UK GDPR and Nigeria's NDPA 2023, focusing on public sector HR operations. By examining UK practices alongside the Nigerian context, it aims to generate actionable recommendations to strengthen HR data governance in Nigeria.

Aim and Objectives of the Study

In undertaking a comparative analysis of the impacts of the UK GDPR and Nigeria's NDPA 2023 on human resource management within the public sector, it is essential to clarify the research objectives that guide the inquiry. First, the study seeks to identify the specific provisions within both regulatory legal frameworks that directly shape HR operations. Second, it examines the adjustments and institutional responses adopted by public sector HR departments in each jurisdiction to ensure compliance with these requirements. Third, the research investigates the persistent challenges and shortcomings that hinder effective implementation of data protection obligations in both contexts. Finally, the study aims to propose strategies for strengthening Nigeria's HR data protection regime by drawing lessons from the United Kingdom's experience and established practices.

Justification of the Study

This study investigates the regulatory requirements of the UK GDPR and Nigeria's NDPA 2023, focusing on safeguarding employee data, strengthening documentation, and responding to data requests. It explores compliance challenges for Nigerian public sector bodies and draws lessons from the UK framework to advance policy, capacity building, and enforcement. The analysis also highlights legal safeguards for employees, empowering them to scrutinize public sector HR practices to foster workplace trust and engagement. By comparing these two regimes, it addresses the limited scholarship on data protection and public sector HR in Nigeria. This research thereby contributes new perspectives to privacy, HR management, and governance studies.

Scope of the Study

This study investigates how public sector bodies in Nigeria and the United Kingdom manage employee data under their respective strong data protection laws, the NDPA 2023 and UK GDPR. It examines HR processes across the employee lifecycle, from recruitment tasks like resume reviews and background checks to maintaining records on salary, progression, and discipline. The research also covers the handling of confidential information, including medical records and health assessments, as well as performance evaluations through monitoring and formal reviews. Specific procedures for secure data storage and deletion during employment terminations are also outlined. The focus is exclusively on public sector organisations, as private companies operate under different practices and regulatory obligations.

Human Resource Management (HRM)

The intersection between Human Resource Management (HRM) and data protection regulations has become a major focus for academic researchers and industry professionals because of its impact on digital transformation initiatives. The research community has conducted numerous studies about HR transformation during the data-driven decision era, which includes automated HR system deployment. Research shows that HR service digitization brings both operational efficiency and new risks for unauthorized employee data access, exploitation, and profiling. Studies indicate HR departments must transform their operational methods to develop compliance-based cultures that safeguard data ethically. Organisations maintain insufficient knowledge about GDPR principles (Bradford, Aboy, and Liddell, 2020) because their non-technical departments, including HR, face challenges in achieving proper compliance, which results in data protection violations.

Human resources professionals face challenges when they try to align GDPR legal needs with their company's operational goals. The collection of personal information during recruitment and workplace monitoring activities creates risks that can lead to privacy rights violations when organisations fail to follow correct procedures. Research shows that HR regulations require updates to match data minimization and purpose limitation standards, which ensure only necessary information gets collected for authorized HR operations. The evaluation of different industries shows that organisations that maintain strong IT-HR partnerships achieve superior data protection compliance results. According to Tursunbayeva et al. (2022), organisations that unite their systems create protected data management systems that operate with automatic authorization tracking and audit trails to maintain legal accountability.

The conventional reactive HR data protection methods face opposition from modern research studies because these studies advocate preventive measures for safeguarding data security. The writing community supports assessment processes that include data protection impact assessments (DPIAs) and encryption technologies and access control mechanisms as fundamental requirements rather than optional choices. Studies about organisations that experienced data breaches showed that inadequate HR data management practices led to increased damage in financial losses and reputation harm. Organisations that integrated data protection regulatory compliance into their strategic HR framework discovered that their employees develop stronger trust, their organisational culture became more resilient, and their regulatory relationships improved. Some experts believe organisations need to train their HR teams about data privacy responsibilities because employing a Data Protection Officer (DPO) alone does not fulfill privacy protection needs, according to Section 32(2)-(3)(a)(c) NDPA 2023; Articles 11 and 12 GAID 2025 and . The literature continuously backs the creation of detailed GDPR training programs, which should address HR requirements to connect theoretical knowledge with practical implementation (Islam, 2023).

Public Sector

The public sector includes all government agencies and their employees. The private sector, on the other hand, includes private businesses, non-governmental organisations, and their employees (Kanapathy, 2016). The public sector of the economy includes all businesses that are owned and run by the government. This includes all kinds of infrastructure, such as bridges, highways, hospitals, and schools. The main goal of the public sector is to offer services that are necessary for the health of society. Usually, these services are free or cost less than normal. Non-profits and other public sector groups do not try to make money. The public sector is very important for society to work well. It gives them the basic services they need for good life. Also, the public sector is very important for the economy's growth and stability. However, the role of the public sector has changed a lot throughout time.

Recent events suggest a transition towards the outsourcing and privatization of public functions. The growth of private companies offering services that were once thought to be public has happened at the same time as the public sector has shrunk (Pollitt and Bouckaert, 2017). Taxes, fees, and fiscal transfers from higher levels of government, such as federal to state governments, are common ways to pay for public services. Governments all throughout the world may use different ways to pay for public services. The public sector establishes partnerships with private sector organisations through which it creates public-private partnerships (P3s). P3s combine different organisational structures to deliver business services and projects that benefit community members. Public sector organisations frequently outsource to obtain goods and services from private companies for their constituents (Kanapathy, 2016).

Human Resources Management in the Public Sector

Human Resource Management (HRM) in the public sector consists of various functions, which include recruitment operations, employee development, payroll administration, personnel documentation maintenance, training, welfare program management, and performance evaluation systems, amongst others. Public corporations are more accountable to citizens than private companies, which makes the following standards like data protection much more important. Public sector human resource management is the use of HRM ideas in the public sector. Public sector human resource management includes hiring, training, paying, and periodically checking on staff. Another strategy to increase the quality of employee work is to lay-off, retrench or sack workers who are not doing their jobs well as corroborated by Babalola (2022).

HRM in the public sector also deals with issues including sexual harassment, workplace diversity, labor conflicts, and welfare benefits. Over the last 20 years, HRM has changed a lot as a field, which has made it more important in businesses today. Lapsley and Wright (2019) say that HRM used to be more of an administrative job than a strategic one that was important for the company's performance. One of the most important things that human resource management does in the public sector is to set up interviews and other ways to hire people. It is their job to design, provide, and manage the logistics of the manpower development for employees who need it. After training, HRM will put the employees where their skill sets are most required and keep an eye on their work

performances to make sure they are doing their best. HRM can fire or move an employee to another department if they are not doing their job well or found most relevant elsewhere, as equally viewed by Lee (2015).

Managing human resources in the public sector deals with a lot of problems, one of which is making the workplace more diverse. Diversity includes a lot of differences between personnel, such as differences in race, gender, sexual orientation, and nationality. The purpose of managing diversity is to stop discrimination and marginalization of minorities. One way to do this is to hire people who represent other groups, or promote diversity culture at the public workplace. For example, the human resources department of a corporation might aim to make sure that there are enough women in management so that everyone has the same chance of getting a job. If attention is not paid to these kinds of problems, the consequences could end up with expensive lawsuits, delays, bad press, and charges of discrimination. Another job that human resources departments in the public sector do is dealing with complaints from employees. Their roles include mediating between a company's management and employees and dealing with grievances in a way that is fair and effective to keep the situation from getting worse (Sharma and Kumar, 2023). For instance, when labour unions want anything from a company's management, they normally go to the human resources department first. In the public sector, human resources management is also in charge of making sure employees are happy and giving them rewards to boost efficiency.

Data Protection and Privacy in HRM

Data protection in human resources functions to protect employees' personal information from any form of malicious use. The process requires organisations to follow legal data handling standards, while they must keep data volumes at their lowest point (*Section 24(1)(b)-(c) NDPA 2023*) apply information strictly according to its original collection purpose, maintain data precision, and delete information after defined storage periods (*Section 24(1)(a), (d)-(f) NDPA 2023*). Organisations lose their business reputation when they fail to follow rules, and employees lose their trust in them. In *Shobna Gulati & others v MGN Ltd* [2015] EWHC 1482 (Ch), substantial damages were awarded to multiple prominent persons for misuse of private information arising from voicemail hacking and related intrusion. The reputational damage, public exposure, and distress were recognized and compensated.

The UK GDPR had a major impact on worldwide HR data management practices for all people. Kuoppamäki and Henttonen (2019) demonstrate how HR departments struggle to meet UK GDPR standards because of employee consent requirements, data reduction rules, and cross-border information transfer rules. The study shows that HR data management needs to stay open and accountable to follow the UK GDPR rules.

Mingers and Walsham (2019) conducted research to understand how employees view data protection practices within human resource systems. The research examines how employee data privacy concerns create conflicts with organisational requirements for data collection and analysis. Research demonstrates that organisations must establish trust-based environments, together with transparency, to reduce staff concerns about HR data management. Multiple studies have identified proper HR data management techniques that protect privacy rights and decrease potential risks. Organisations must conduct data protection impact assessments and implement privacy-by-design principles and train employees regularly about data privacy requirements (Wright et al., 2020).

Privacy laws, including UK GDPR, create rules for organisations to establish their HR analytics data usage protocols. The research study by Rasmussen and Ulrich (2020) explores the obstacles that HR analytics experts encounter when they try to stay compliant while extracting valuable information from employee data. Research findings indicate that businesses must unite their data-driven decision processes with privacy protection systems to fulfill legal requirements. Organisations require HR technology solutions to maintain compliance with privacy regulations. The research by Strohmeier et al. (2019) investigates how HR technology platforms protect data privacy and security compliance. The research demonstrates that HR data security depends on three main factors, which include encryption methods, access restrictions, and audit trail systems for protection.

Castiglione et al. (2021) present in their study that employee trust in HR departments determines their readiness to follow privacy policies. The study investigates how organisational beliefs about transparency and equity,

together with communication methods, affect employee adherence to data privacy regulations. Organisations need to build trust as their base foundation, according to research findings, because it serves as the core requirement for developing responsible and compliant human resources data management systems. Ethical issues are of utmost importance in HR data management practices. Meszaros et al. (2018) examine the ethical dilemmas faced by HR professionals in balancing organisational objectives with individual privacy rights. The research emphasizes the need for ethical leadership and decision-making frameworks in guiding HR data management techniques.

UK GDPR Overview

The UK GDPR operates through seven fundamental principles, which include legality and fairness, openness, purpose limitation, data minimisation, accuracy, integrity/confidentiality, and responsibility. The HR industry bases legal processing on contract performance and legal obligations rather than obtaining consent for processing activities. The Information Commissioner's Office (ICO) functions as the organisation that enforces all existing regulations. The UK GDPR shows how American privacy rules for personal information differ from European Union data protection regime (*Google Spain SL v AEPD and Mario Costeja González* (C-131/12, CJEU, 2014); *Copland v United Kingdom* (2007) ECHR 62617/00). The new law replaced the EU Data Protection Directive along with the UK's Data Protection Act and started its implementation on May 25, 2018. All businesses that handle personal information from EU residents must follow these rules. The rule applies to data controllers and processors equally while operating without any territorial restrictions. The most the corporation can be fined is 20 million euros, or 4% of its yearly worldwide sales, whichever is more.

Both EU and the UK GDPR appear similar save for the facts that the UK GDPR contains provisions on national security, intelligence services and immigration, with ICO being the regulator as against the European Data Protection Board (EDPB). 13 years is adopted as age of consent while it is 16 years in the EU. There are other amendments that distinguish the two laws substantially. The data protection legal regime in the UK is supplemented with the Data Protection Act 2018, Privacy and Electronic Communications (EC Directive) Regulations 2023, Data (Use and Access) Act 2025, etc.

The law grants compensation rights to data owners who experience theft of their information. The GDPR establishes specific rules for personal data management, which require organisations to obtain consent before data collection and to defend the privacy rights of data subjects. Article 9 of the UK GDPR protects personal data, which includes racial information and ethnic background, political opinions, religious beliefs, trade union status, genetic information, biometric data, health records, and sexual orientation. The UK GDPR establishes in Article 6(4) that data controllers must follow specific requirements before they can authorize new researchers to access an existing dataset. The institutions needed to adjust their data collection, recording, storage and sharing methods because of this change.

The law requires data to remain removable according to the UK GDPR, which functions to give users control over their data through worldwide regulations that manage organisations that store and handle personal information. The GDPR prohibits the storage of personal data on blockchain systems because the removal of encryption keys does not fulfill the requirements for data deletion (Herian, 2018). The European Union member states' data protection authorities have not started enforcing the rules because they lack financial resources, and the rules are challenging to enforce across borders; the industry shows no signs of cooperation. The European Union established rules that prevent personal data transfers from its member states to nations that do not maintain sufficient privacy protection standards (Brown and Marsden, 2013). The European Commission has the task of performing the "adequacy" evaluation, which requires foreign nations to adopt multiple key protections from EU data privacy directives and regulations into their national legal systems.

Nigeria Data Protection Act (NDPA) 2023 Overview

The NDPA 2023 establishes new data rights for citizens, creates stricter compliance requirements, and appoints the NDPC as the official regulatory body. The government agency monitors HR operations through its employee data protection system, which includes penalty systems for rule violations. The Nigerian government achieved a major victory in privacy protection through the passage of the NDPA in June 2023. People expressed doubts

about Nigeria's data protection policy before this because many thought it lacked proper safeguards and failed to provide meaningful protection. Its force of enforcement was weak because of enactment status as a soft law. Regulation in Nigeria is a subordinate legislation and not comparable to act of the parliament. Nigeria has maintained a fragmented and inadequate approach to data protection through its historical legal framework. The National Information Technology Development Agency (NITDA) introduced the Nigeria Data Protection Regulation (NDPR) in 2019 (Babalola, 2022). The legislation created an important foundation, yet it failed to establish a complete set of legal protections for data privacy. People expressed their dissatisfaction about the NDPR because it failed to cover enough areas, and its enforcement process was too strict (Aloamaka, 2023).

The NDPA seeks to establish a solid legal system for personal data protection through which it follows the EU GDPR framework. People throughout the world think of the GDPR as the best data privacy law. The law has created a major impact on the National Data Protection Authority (NDPA). The NDPA contains multiple provisions from the General Data Protection Regulation (GDPR) that protect personal data through accountability measures, data subject rights, and transparency requirements. The legal norm transfer seeks to improve Nigerian data protection standards through international benchmark alignment, which will build trust among data subjects and boost Nigeria's position in the worldwide digital market. The NDPA wants to fix the problems with past legislation by giving data controllers and processors clear definitions, duties, and responsibilities (Aloamaka, 2025). The law establishes various safeguards for personal information through mandatory consent protocols and breach notification requirements, and it establishes the Nigeria Data Protection Commission (NDPC) to oversee rule enforcement.

Institutional Theory

The study of public sector organisational adaptation to social and legal requirements and regulatory demands receives essential support from institutional theory. The theory shows that organisations operate based on efficiency goals and institutional requirements, which help them maintain their legitimacy, stability, and survival (DiMaggio and Powell, 1983). The research shows that public sector HR departments modify their behavior through institutional pressures that stem from data protection rules, including Nigeria's NDPA 2023 and UK GDPR. Public organisations maintain these rules because they serve to protect against problems and show their responsibility to the public while following international governance standards.

Scott (2014) explains that institutional theory rests on three fundamental components, which include moral forces, cultural-cognitive elements, and regulative mechanisms. The cultural-cognitive pillar functions as a system of common public beliefs and social norms that support workers' rights to privacy and fair treatment. The normative pillar contains professional standards and ethical values, which include proper methods for protecting employee information. The regulative pillar contains official guidelines and penalties, which in this research study include the GDPR and NDPA legal requirements.

The UK public sector HR departments probably achieved better GDPR compliance because of powerful institutional requirements, effective enforcement systems, and strong data privacy values. Nigerian public sector organisations continue their transition process because they encounter difficulties in implementing NDPA 2023 due to insufficient knowledge, weak enforcement mechanisms, and inadequate resource availability. The institutional theory serves as an appropriate framework to study the differences between these rules. The research shows that UK and Nigerian HR practices differ because of legal differences and institutional factors that affect compliance levels.

Empirical Studies on GDPR Compliance Effectiveness

Recent empirical studies demonstrate that UK GDPR provides effective protection for employee privacy during actual workplace operations. Christensen et al. (2021) studied privacy event patterns at 200 European organisations during the complete UK GDPR implementation period. The researchers discovered that employee data breach reports dropped by 31% during the three years after GDPR implementation. The statistics show that HR organisations have achieved major advancements in safeguarding personal information. The research by Politou et al. (2020) showed that employees do not understand their privacy rights and proper usage of these rights, even though organisations invest large amounts of money in GDPR compliance systems. The

"implementation gap" proves that technological compliance by itself does not protect worker privacy. A recent study by Veale and Binns (2017), Bogiatzis-Gibbons, D., etal. (2023) on data protection impact assessments (DPIAs) in HR contexts found that many businesses adopt cursory evaluations that ignore real privacy risks. The authors examined 50 HR-related DPIAs to discover that 82% of them failed to incorporate employee feedback, while 68% lacked proper risk control measures (Birnhack, 2008).

Organisations now use technology to meet UK GDPR requirements for their HR system operations, according to growing academic research within contemporary literature. According to Garcia-Arroyo and Osca (2021), the Privacy by Design framework started with Robinson et al. (2009), who Schaar (2010) later adapted for human resources system development. According to Malgieri and Custers (2018), organisations face multiple challenges when they attempt to implement automated decision-making protection systems in HR systems under GDPR Article 22. The research findings showed that current HR technology systems lack the necessary features to comply with GDPR requirements across multiple domains (Birnhack, 2008). The research found that many organisations maintain systems that do not follow the transparency and explain ability requirements set by the GDPR. Academic researchers have studied cloud computing adoption for human resource management systems in multiple studies. Tikkinen-Piri et al. (2018) studied present GDPR compliance challenges for HR data processing in cloud systems, yet Pearson and Benameur (2010) developed privacy protection models for cloud-based HR systems.

Healthcare organisations face particular challenges in safeguarding HR data because their processing systems manage employment records together with patient information. Terry's study from 2017 revealed that healthcare organisations encounter multiple difficulties when they attempt to follow GDPR and industry standards for managing worker data because 78% of healthcare organisations reported problems with occupational health monitoring and incident reporting requirements. According to Finck and Pallas (2020), financial services organisations encounter equivalent challenges. The study revealed that financial sector HR departments need to follow GDPR requirements together with all existing employee monitoring regulations, which aim to prevent financial crimes and market misconduct. Educational institutions operate under a different set of rules when compared to other organisations. The research team of Hoel and Chen (2019) determined that university HR departments encounter particular obstacles because of academic freedom and research activities, and student work arrangements, which need tailored GDPR compliance solutions.

Research Design

This study implements a mixed methods approach to data collection, which combines quantitative and qualitative methods for analysis. The study demands mixed methods because it needs to examine both legal and policy aspects of Nigeria's NDPA 2023 and UK GDPR and their real-world implementation in public sector HR departments. The document review section evaluates the legal and regulatory aspects of the two frameworks by examining their contents and their influence on HR management practices (Teddlie and Tashakkori, 2009). The questionnaire survey provides actual data about HR manager' knowledge levels and their compliance with rules and their challenges in both legal systems. The research study achieves result validity through this combination because it applies multiple methods to collect data (Braun and Clarke, 2019). The research investigates theoretical elements and practical applications of the subject matter.

Population of the Study

The study includes two main population groups for its analysis. The research group contains HR managers/officers and compliance officers who operate within public sector organisations (Board, ministries, parastatals and agencies) across Nigeria and the United Kingdom. The selection was informed because their work involves handling employee information and ensuring staff protection of personal data according to legal requirements. The secondary population consists of legal documents together with annual reports, policy guidelines, regulatory frameworks, and enforcement decisions from regulatory bodies, including the NDPC and the UK Information Commissioner's Office (ICO). The research maintains its findings according to standard legal criteria and actual data through its evaluation of human participants and documented evidence (Creswell and Creswell, 2018).

Sampling Technique and Sample Size

The study implemented a purposive sampling method to gather data. The study needs information from professionals who handle data protection compliance and human resources management because they possess the essential knowledge and responsibilities to address the research subjects. The research collected data through questionnaires from two groups of participants, who include 50 human resources officers based in the UK and 50 human resources officers based in Nigeria. The selection of fifty responders from each country maintains equilibrium because not all participants were expected to respond. The research selected documents through purposive sampling, including only HR data protection materials, which consist of UK GDPR full text, NDPA 2023, ICO recommendations, and NDPC compliance frameworks.

Sources of Data

This investigation depended on primary and secondary sources, which functioned as its main information providers. The research collected primary data by distributing structured questionnaires to HR professionals who operate within public sector organisations in Nigeria and the UK. The survey aimed to determine public knowledge about data protection and their compliance strategies, their perception of main obstacles, and their actual experiences with data protection law enforcement. Secondary data was obtained through an in-depth review of legislative documents, policy guidelines, regulatory reports, and academic research materials. The two-pronged method unites authentic legal documents with practical experiences from fieldwork to generate research findings (Bryman, 2016).

Research Instruments

This research relied on two main tools for data collection. The survey contained two types of questions, which included multiple answer options and single answer options. The open-ended questions allowed respondents to describe their habits and problems through qualitative answers, but the closed-ended questions used multiple-choice answers and a Likert scale to produce numerical data (Johnson and Onwuegbuzie, 2004). The second tool is a document review checklist, which helped with the systematic analysis of legal and regulatory materials. The checklist focused on employee data rights and processing rules, accountability systems, and HR compliance requirements according to the NDPA 2023 and the UK GDPR.

Method of Data Collection

The method for data collection proceeded through two distinct phases. The initial round of the process required HR officers to receive their questionnaires through email and Google Forms, which function as online survey tools. This method operates as a cost-effective solution that helps people from different nations to connect. The questionnaire remained available to participants for two weeks, during which they received reminder messages after seven days to boost their participation rates. The second step required document review, which demanded precise collection of policy documents, legal texts, and regulatory reports from academic databases and official sources, including NDPC and ICO websites.

Method of Data Analysis

A mixed technique was utilized to analyze the data. The study applied descriptive statistics to process the survey data by using frequencies and percentages and mean scores. The analysis enabled the identification of patterns that show how people understand and follow rules and what challenges they encounter between the two countries. The research applied thematic analysis to examine the qualitative data, which contains material assessment results and open-ended response answers (Saunders, Lewis, and Thornhill, 2019). Various themes were identified and explored, which include HR effects and employee rights, institutional barriers, and compliance strategies. The investigation of data privacy laws on HR operations benefits from merging two research results through a convergent mixed methods strategy, which united statistical and narrative data interpretation.

Ethical Considerations

The research followed all established ethical guidelines that govern social scientific investigation. The data collection process began after all respondents gave their informed consent. The questionnaire survey allowed participants to join at their own free will. The study participants were assured of confidentiality protection, together with anonymity, and the final report removed all personal information. The information gathered remained protected in secure storage facilities to support academic research activities. The evaluation process for documents operated with content that exists in the public domain and meets legal requirements to safeguard intellectual property rights (Silverman, 2020).

RESULTS AND DISCUSSION

Introduction

This section examined the study's findings about the comparative impacts of the UK GDPR and Nigeria's NDPA 2023 on human resource management (HRM) in the public sector. The results were obtained from primary data (questionnaire responses from HR officers in selected public sector businesses in the UK and Nigeria) and secondary data (document analyses of GDPR and NDPA regulations, compliance reports, and relevant literature). The analysis utilized a theme framework, aligning responses with the study objectives.

Awareness and Understanding of Data Protection Laws

The study revealed that HR managers who work within the UK public sector achieve a superior understanding of GDPR rules. Participants demonstrated awareness of essential requirements, including employee consent, data minimization, and the right to deletion. This aligns with the observations of Christensen, Hansen, and Andersen (2021), who indicated that GDPR has been integrated into the HR compliance culture after three years of implementation. On the other hand, the NDPA 2023 is not very well known in the Nigerian public sector. The majority of HR staff indicated they understood the rule, yet they struggled to determine its practical meaning. The findings support Islam (2023), who states that implementing human resources strategies remains difficult in developing nations because they lack sufficient resources and expert personnel.

Implementation Practices in HR Data Management

The UK demonstrated GDPR compliance through organized HR systems, which include anonymizing employee records and setting exact data retention limits and full disclosure of subject access request procedures. The document review process showed consistency with previous studies, which proved UK GDPR implementation brought major changes to HR operations (Tikkinen-Piri et al., 2018). Nigerian HR managers encountered difficulties when they tried to apply similar procedures because their organisation lacked proper technical systems, administrative structure, organisational arrangement and staff training programs. The research results align with Sharma and Kumar (2023) because organisations that employed data protection officers achieved superior compliance outcomes compared to those that lacked these systems.

Employee Rights and Privacy Protection

The UK GDPR establishes strict employee data protection, which grants workers the ability to access their personal information and modify or delete it. The UK workforce believes that these rights have enhanced worker confidence in HR operations. The research findings align with Malgieri and Custers (2018), who stated that people now view personal data as a valuable asset that could be measured. Human resource operations in Nigeria lack proper protection for employees' rights to erase data and transfer information. HR managers in large numbers stated these rights exist only as dreams because they do not receive any implementation. The document analysis showed that NDPA 2023 contains insufficient enforcement provisions, which Terry (2017) also identified as a problem for healthcare data regulatory arbitrage.

Institutional Pressures and Compliance

The research study applied institutional theory to explain variations in organisational compliance patterns. Studies demonstrate that public sector organisations in the UK experience strong institutional demands. The organisation must follow professional HR standards while being subject to ICO oversight and public examination. The pressures lead organisations to copy each other's compliance methods, which results in isomorphic behaviors (DiMaggio & Powell, 1983; Scott, 2014). However, Nigerian institutions face reduced enforcement and normative pressures, leading to fragmented compliance approaches. This exemplifies Suchman's (1995) claim that legitimacy, rather than efficiency, often dictates organisational acceptance of regulatory practices.

Challenges in Compliance

People in both countries saw problems, but they had different priorities. In the UK, problems arise from balancing employee surveillance with privacy (Bradford, Aboy, & Liddell, 2020), as well as the costs of setting up privacy-by-design frameworks (Schaar, 2010). Nigerian respondents explained that employees lack sufficient training because organisations do not allocate enough money to protect their human rights information systems, and workers do not understand their rights. The research of Politou et al. (2020) shows that organisations encounter major challenges when they attempt to harmonize their technological constraints, including data backup systems, with the UK GDPR requirement to erase personal information, which produced GAID 2025.

The research shows that the UK established a compliance-oriented HR system through GDPR, yet Nigeria continues to develop its institutional framework under NDPA 2023. The United Kingdom maintains its human resources departments at high operational standards because institutional power exists alongside a system of accountability. Human resource managers in Nigeria face two major obstacles because they must operate with insufficient resources and weak regulatory systems. The study results support previous findings from Garcia-Arroyo and Osca (2021) and Tursunbayeva et al. (2022), which show big data and people analytics create advantages and ethical problems for HR when data protection systems remain weak.

CONCLUSION

This study examined the influence of the UK GDPR and Nigeria's NDPA 2023 on public sector human resource management practices. Employing a mixed-methods approach, the findings indicated that UK GDPR has profoundly impacted HR procedures in the UK, integrating compliance mechanisms into recruitment, personnel management, and employee monitoring practices. The NDPA 2023 legislation in Nigeria exists at an early stage of development, which creates difficulties for HR departments because they lack sufficient understanding and resource availability, and the necessary competencies to implement it (Mantelero, 2019).

The study showed that institutional forces play a major role in determining how HR compliance functions. The UK environment contains various regulatory and cultural elements that force HR departments to integrate GDPR requirements into their core operational procedures. The Nigerian system encounters variable compliance because the authorities lack proper enforcement mechanisms, and professional standards remain below acceptable levels. The study showed that UK workers obtain better protection of their rights through GDPR, yet Nigerian workers remain unaware of how their data gets collected and processed (Christensen et al., 2021).

The research demonstrates that organisations need more than solid legal frameworks to achieve HR compliance with data privacy requirements. The system depends on four main components: The organisational structure, employee knowledge levels, enforcement system, and the workplace culture. The United Kingdom showed that achieving long-term compliance demands clear legal rules together with strong institutional backing. Nigeria made progress through the NDPA 2023, which is being enhanced by GAID 2025, but the system needs to become more institutionalised to reach its full potential (Sharma and Kumar, 2023).

Institutional theory analysis revealed which factors create various compliance patterns across different organisational environments. HR managers follow data protection protocols because these guidelines help them

meet legal requirements, maintain organisational credibility, and protect public trust. People tend to follow rules more when institutional power is at a high level, yet they tend to break rules when institutional power weakens.

RECOMMENDATIONS

The following recommendations are made based on the results:

Strengthening Institutional Capacity in Nigeria: Nigeria needs to build institutional strength by ensuring public sector organisations appoint data protection officers and allocate funds for staff education and technology system enhancement.

Employee Awareness Campaigns: Nigerian Human Right departments need to allocate resources for staff education about their rights according to NDPA 2023 because this approach mirrors the UK GDPR awareness initiatives.

Policy Harmonization and Guidance: The Nigerian Data Protection Commission needs to create specific HR compliance guidelines that mirror UK GDPR codes of practice to help organisations follow legal requirements when dealing with HR data management (Team, 2025).

Using Privacy by Design: Both countries must establish HR information systems that include privacy protections security from their initial design because health and performance data require special protection.

Comparative Learning: The UK offers useful models for Nigerian policymakers to protect worker rights, but UK officials need to study Nigerian methods for managing new technological developments through proper regulatory systems.

Further Research: Future research needs to study the commercial sector to understand how AI and big data analytics will affect HR compliance with data protection rules.

REFERENCES

CASE LAW

United Kingdom and European Case Law

1. Bekoe v Islington LBC [2023] EWHC 1668 (KB).
2. Copland v United Kingdom (2007) ECHR 62617/00
3. Google Spain SL v Agencia Española de Protección de Datos (AEPD) (C-131/12) [2014] ECLI:EU:C:2014:317.
4. R (Public Law Project) v Lord Chancellor [2016] UKSC 39.
5. R v Secretary of State for the Environment, ex parte Spath Holme Ltd [2001] 2 AC 349.
6. Raine v JD Wetherspoon Plc [2025] EWHC 1593 (KB).
7. S. and Marper v. The United Kingdom (2008) ECHR 1581.
8. Shobna Gulati & others v MGN Ltd [2015] EWHC 1482 (Ch).

Nigerian Case Law

1. A.-G. Federation vs. A.-G. Abia & Ors (No. 2) (2002) 6 NWLR (Pt. 764) 542.
2. Chief Obafemi Awolowo vs. Alhaji Shehu Shagari & 2 Others (1979) All N.L.R 105.
3. Dangana vs. Usman (2013) 6 NWLR (Pt. 1349) 50.
4. Incorporated Trustees of Digital Rights Lawyers Initiative & ORS vs NIMC (2021) LPELR-55623(CA).
5. The Incorporated Trustees of Paradigm Initiative for Information Technology Development & Ors vs the Attorney General of the Federation & Ors (CA/L/556/2017).

Legislation

European Union

1. European Parliament and the Council (2016) Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L 119/1.

Nigeria

2. General Application and Implementation Directive 2025
3. Nigeria (2019) Nigeria Data Protection Regulations 2019.
4. Nigeria Data Protection Act 2023.

United Kingdom

1. Data (Use and Access) Act 2025
2. Data Protection Act 2018 (c. 12)
3. Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426)
4. United Kingdom General Data Protection Regulations

Journals, Books, Reports And Online Resources

1. Aloamaka, P.C. (2023) 'Data protection and privacy challenges in Nigeria: Lessons from other jurisdictions', UCC Law Journal, 3, pp. 281–300.
2. Aloamaka, P.C. (2025) 'A critical anal ysis of the Nigeria Data Protection Act 2023: Elevating standards to global norms', UCC Law Journal, 4(2), pp. 242–263. doi:10.47963/ucclj.v4i2.1724 (Accessed on 21/09/2025).
3. Babalola, O. (2022) 'Nigeria's data protection legal and institutional model: An overview', International Data Privacy Law, 12(1), pp. 44–56.
4. Birnhack, M.D. (2008) 'The EU Data Protection Directive: An engine of a global regime', Computer Law & Security Review, 24(6), pp. 508–520.
5. Bogiatzis-Gibbons, D., Charles, L., Dewing, H., Gretschel, C., Jomy, M., Reid, A. & Slack, R. (2024) 'A literature review on bias in supervised machine learning'. Research note, Financial Conduct Authourity, 11 December, Available at: https://www.fca.org.uk/publication/research-notes/literature-review-bias-in-supervised-machine-learning.pdf (Accessed: 30 July 2025).
6. Bradford, L., Aboy, M. and Liddell, K. (2020) 'COVID-19 contact tracing apps: A stress test for privacy, the GDPR, and data protection regimes', Journal of Law and the Biosciences, 7(1), lsaa034.
7. Braun, V. and Clarke, V. (2019) 'Reflecting on reflexive thematic analysis', Qualitative Research in Sport, Exercise and Health, 11(4), pp. 589–597. doi:10.1080/2159676X.2019.1628806 (Accessed on 19/09/2025).
8. Bryman, A. (2016) Social research methods. 5th edn. Oxford: Oxford University Press.
9. Castiglione, A., Castro, L. and Oliveira, T. (2021) 'Privacy in the workplace: Employees' trust in HR and their compliance with privacy policies', Journal of Business Research, 123, pp. 198–209.
10. Christensen, L., Hansen, K. and Andersen, P. (2021) 'GDPR impact assessment: Three years of employee data protection in practice', European Journal of Law and Technology, 12(2), pp. 1–28.
11. Creswell, J.W. and Creswell, J.D. (2018) Research design: Qualitative, quantitative, and mixed methods approaches. 5th edn. Thousand Oaks, CA: Sage Publications.
12. DiMaggio, P.J. and Powell, W.W. (1983) 'The iron cage revisited: Institutional isomorphism and collective rationality in organisational fields', American Sociological Review, 48(2), pp. 147–160. doi:10.2307/2095101 (Accessed on 20/08/2025).
13. Finck, M. and Pallas, F. (2020) 'They who must not be identified—Distinguishing personal from non-personal data under the GDPR', International Data Privacy Law, 10(1), pp. 11–36.

14. Garcia-Arroyo, J. and Osca, A. (2021) 'Big data contributions to human resource management: A systematic review', The International Journal of Human Resource Management, 32(20), pp. 4337–4362.
15. Hoel, T. and Chen, W. (2019) 'Privacy-driven design in learning analytics research practice: Exploring the design space', Computers & Education, 130, pp. 139–151.
16. Islam, M. (2023) Analyzing and enhancing compliance and regulatory affairs in HR: A comprehensive study on policy adherence and legal frameworks.
17. Johnson, R.B. and Onwuegbuzie, A.J. (2004) 'Mixed methods research: A research paradigm whose time has come', Educational Researcher, 33(7), pp. 14–26.
18. Kanapathy, K. (2016) 'The relevance of new public management in the South African public sector', African Journal of Public Affairs, 9(2), pp. 11–26.
19. Kuoppamäki, S.M. and Henttonen, K. (2019) 'Managing personal data at work: Employee perceptions and the role of human resource management', Employee Relations, 41(3), pp. 622–639.
20. Lapsley, I. and Wright, C. (2019) Public sector accounting, accountability and austerity. London: Routledge.
21. Lee, E.J. (2015) 'Competency-based human resource management in public sector organisations', Public Personnel Management, 44(4), pp. 453–469.
22. Malgieri, G. and Custers, B. (2018) 'Pricing privacy – The right to know the value of your personal data', Computer Law & Security Review, 34(2), pp. 289–303.
23. Mantelero, A. (2019) 'AI and big data: A blueprint for a human rights, social and ethical impact assessment', Computer Law & Security Review, 34(4), pp. 754–772.
24. Meszaros, P.S., Sabherwal, R. and Deokar, A.V. (2018) 'Ethical and legal considerations of big data in human resources management', Journal of Organisational Computing and Electronic Commerce, 28(4), pp. 266–286.
25. Mingers, J. and Walsham, G. (2019) 'Towards ethical information systems: The contribution of discourse ethics', MIS Quarterly, 43(4), pp. 1203–1223.
26. Pearson, S. and Benameur, A. (2010) 'Privacy, security and trust issues arising from cloud computing', IEEE Second International Conference on Cloud Computing Technology and Science, pp. 693–702.
27. Politou, E., Michota, A., Alepis, E., Pocs, M. and Patsakis, C. (2020) 'Backups and the right to be forgotten in the GDPR: An uneasy relationship', Computer Law & Security Review, 38, 105442.
28. Pollitt, C. and Bouckaert, G. (2017) Public management reform: A comparative analysis – Into the age of austerity. Oxford: Oxford University Press.
29. Rasmussen, T. and Ulrich, D. (2020) 'Ethics and HR analytics: Building a framework for fairness and privacy in practice', Human Resource Management Review, 30(1), 100677.
30. Saunders, M., Lewis, P. and Thornhill, A. (2019) Research methods for business students. 8th edn. Harlow: Pearson.
31. Schaar, P. (2010) 'Privacy by design', Identity in the Information Society, 3(2), pp. 267–274.
32. Scott, W.R. (2014) Institutions and organisations: Ideas, interests, and identities. 4th edn. Thousand Oaks, CA: Sage Publications.
33. Sharma, A. and Kumar, R. (2023) 'HR data protection officers: A comparative analysis of organisational privacy outcomes', International Journal of Human Resource Management, 34(8), pp. 1547–1572.
34. Silverman, D. (2020) Interpreting qualitative data. 6th edn. London: Sage Publications.
35. Strohmeier, S., Heinzl, A. and Rothlauf, F. (2019) 'Unravelling the dark side of HRIS: A qualitative analysis of employee reactions towards the introduction of electronic monitoring systems', European Journal of Information Systems, 28(5), pp. 482–505.
36. Swire, P.P. and Lagos, J. (2020) 'The California Consumer Privacy Act of 2018 and the GDPR: Core differences and operational impacts for privacy regulation of business', Journal of Law and Policy, 29(1), pp. 127–157.
37. Team, I.G.P. (2025) EU general data protection regulation (GDPR): An implementation and compliance guide. Birmingham: Packt Publishing Ltd.
38. Teddlie, C. and Tashakkori, A. (2009) Foundations of mixed methods research: Integrating quantitative and qualitative approaches in the social and behavioral sciences. Thousand Oaks, CA: Sage Publications.
39. Terry, N.P. (2017) 'Regulatory disruption and arbitrage in healthcare data protection', Yale Journal of Health Policy, Law, and Ethics, 17(1), pp. 143–208.

40. Tikkinen-Piri, C., Rohunen, A. and Markkula, J. (2018) 'EU General Data Protection Regulation: Changes and implications for personal data collecting companies', Computer Law & Security Review, 34(1), pp. 134–153.
41. Tursunbayeva, A., Pagliari, C., Di Lauro, S. and Antonelli, G. (2022) 'The ethics of people analytics: Risks, opportunities and recommendations', Personnel Review, 51(3), pp. 900–921.
42. Veale, M. and Binns, R. (2017) 'Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data', Big Data & Society, 4(2), pp. 1–15. doi:10.1177/2053951717743530 (Accessed on 11/09/2025).
43. Wright, D., Jalloh, A.M., Wright, K. and Yerby, J. (2020) 'A framework for ensuring privacy and data protection in HR management', Business Horizons, 63(4), pp. 495–504.