

Data Privacy and Ethical Challenges in the Management of Migrant Records in Nigeria¹

Ugonna Vivian Ailakhu¹ & Smart Eromosele Ambrose²

^{1&2} Department of Library and Information Science
Faculty of Education
National Open University of Nigeria
Abuja

Corresponding author's email: vailakhu@noun.edu.ng

Abstract

The management of migrant records in Nigeria has become a vital component of migration governance, national security, and human rights protection. This study investigates the ethical and privacy concerns surrounding the collection, processing, and storage of migrant data within Nigeria's migration management systems. It demonstrates how agencies such as the Nigeria Immigration Service (NIS), the National Identity Management Commission (NIMC), and the National Commission for Refugees, Migrants, and Internally Displaced Persons (NCFRMI) handle sensitive information, including biometric data, travel histories, and refugee documents. Even though the Nigerian Data Protection Act has been signed into law, substantial ethical issues remain, particularly in terms of data protection, consent, secrecy, and responsibility. The study demonstrates that frequent breaches, unauthorised sharing, and misuse of migrant information are driven by inadequate cybersecurity infrastructure, a lack of institutional cohesion, and a lack of education about data ethics. It also discusses the conflict between national security needs and individual privacy rights, emphasising that ineffective enforcement and oversight lead to ethical issues. The paper emphasises the importance of a human rights-based and moral framework for the control of migrant data in Nigeria. According to the study, robust legislation alone is insufficient to ensure open, safe, and accountable migration management. It should also include ethical standards, professional training, and institutional improvements that prioritise privacy, dignity, and fairness when handling migrant data.

Keywords: Data Protection Act, migration governance, ethics, human rights, and migrant records

¹ DOI: <https://doi.org/10.82265/s33f-k758>

Protection des données et enjeux éthiques dans la gestion des dossiers des migrants au Nigéria

Résumé

La gestion des dossiers des migrants au Nigéria est devenue un élément essentiel de la gouvernance migratoire, de la sécurité nationale et de la protection des droits humains. Cette étude examine les enjeux éthiques et les questions de protection de la vie privée liés à la collecte, au traitement et au stockage des données des migrants au sein des systèmes de gestion migratoire du Nigéria. Elle analyse la manière dont des institutions telles que le Nigeria Immigration Service (NIS), la National Identity Management Commission (NIMC) et la National Commission for Refugees, Migrants and Internally Displaced Persons (NCFRMI) traitent des informations sensibles, notamment les données biométriques, les historiques de voyage et les documents relatifs aux réfugiés. Bien que la loi nigériane sur la protection des données (Nigeria Data Protection Act) ait été adoptée, d'importants défis éthiques persistent, notamment en matière de protection des données, de consentement, de confidentialité et de responsabilité institutionnelle. L'étude met en évidence que les violations fréquentes, le partage non autorisé et l'utilisation abusive des données des migrants sont favorisés par l'insuffisance des infrastructures de cybersécurité, le manque de coordination institutionnelle et une faible sensibilisation aux principes d'éthique des données. Elle examine également les tensions entre les impératifs de sécurité nationale et le respect du droit à la vie privée, en soulignant que les lacunes dans l'application des lois et les mécanismes de contrôle contribuent à l'émergence de ces défis éthiques. L'article insiste sur la nécessité d'adopter un cadre normatif fondé sur les droits humains et l'éthique pour la gestion des données migratoires au Nigéria. Il soutient que l'existence de cadres juridiques robustes, à elle seule, ne suffit pas à garantir une gouvernance migratoire transparente, sécurisée et responsable. Elle doit être complétée par l'élaboration de normes éthiques, la formation professionnelle et le renforcement institutionnel, afin de garantir le respect de la vie privée, de la dignité et de l'équité dans le traitement des données des migrants.

Mots-clés : Protection des données, gouvernance migratoire, éthique, droits humains, dossiers des migrants.

INTRODUCTION

The management of personal information has become a critical component of contemporary information governance, particularly where sensitive human data is collected and maintained across institutions. In recent years, increasing attention has been paid to data privacy and ethical responsibilities among policymakers and information professionals, who expect institutions that handle human records to ensure confidentiality, transparency, accountability, and the protection of individual rights, especially for vulnerable populations. Migration has significantly expanded the scope of personal data collection, as governments and international organisations maintain extensive records for identification, migration control, humanitarian support, and policy planning. In Nigeria, the growing movement of people across borders has made the management of migrant information an essential aspect of migration governance, with agencies increasingly relying on digital systems and biometric technologies to monitor migration flows, enhance national security, and provide humanitarian services. While these technological systems improve administrative efficiency, they also raise serious ethical and privacy concerns, as migrant records often contain highly sensitive information, such as biometric data, travel histories, and identity documentation. Globally, there is a growing emphasis on balancing national security interests with migrants' rights to privacy and dignity, yet challenges such as unauthorised data sharing, weak cybersecurity infrastructure, and inadequate oversight continue to raise ethical questions about consent, confidentiality, and institutional accountability. Within this context, the management of migrant records presents complex governance challenges that require stronger ethical frameworks and data protection mechanisms to ensure that migrant information is handled responsibly, securely, and with respect for human rights.

Data privacy and ethics are fundamental principles in the responsible collection, processing, storage, and use of personal information in both public and private sectors. Globally, modern data protection frameworks emphasise core principles such as lawfulness, fairness, transparency, purpose limitation, data minimisation, accountability, and security in the handling of personal data (Voigt & Von dem Bussche, 2017; Paul, 2024; Johnson, 2020). These principles require that organisations collect only the data necessary for a legitimate purpose, process it with the consent or knowledge of the data subject, and protect it from unauthorised access, misuse, or disclosure. The concept of data minimisation, for example, emphasises that only essential personal information should be collected to reduce risks such as identity theft or data misuse (Gonzalez & Staddon, 2021). Ethical data management also demands

transparency and fairness in decision-making processes, ensuring that personal data is not used to discriminate against individuals or groups and that individuals retain control over their personal information (Ndukwe, 2022).

Within the context of migration governance, the ethical management of migrants' records is particularly sensitive because such records often contain biometric, demographic, and legal information that can affect an individual's security, legal status, and access to services. In Nigeria, data protection has increasingly been guided by the Nigeria Data Protection Act (2023) and earlier regulatory frameworks, emphasising lawful processing, informed consent, and secure storage of personal information by both public and private institutions (Nigeria Data Protection Commission, 2023; Adeleke & Ojo, 2023). Similarly, in South Africa, the Protection of Personal Information Act, 2013 (POPIA) establishes strict requirements for the lawful processing of personal data and the protection of individuals' privacy rights, including migrants and foreign residents (Government of South Africa, 2013). Globally, many countries align their data protection frameworks with standards like the General Data Protection Regulation (GDPR), promoting strong safeguards for personal data and accountability in its management (Voigt & Von dem Bussche, 2017). These regulatory frameworks highlight the importance of ethical governance in migration data systems, ensuring that migrants' records are managed securely, used only for legitimate administrative or humanitarian purposes, and protected from exploitation, discrimination, or unauthorised surveillance (Gonzalez & Staddon, 2021).

Migration in West Africa, particularly Nigeria, is influenced by political, economic, and historical factors. Labour demand, commerce, environmental changes, and violence account for around 70% of migrant movements in the region (International Organisation for Migration, 2025). Colonial laws disrupted traditional migration patterns that previously facilitated commerce and urbanisation. Following independence, Nigeria emerged as a major migration destination and source country, facilitated by ECOWAS frameworks that allow free movement and residency rights (Chukwuma & Hassan, 2024). Annually, millions travel to and from Nigeria for economic, environmental, and security-related reasons. More than three million people have fled to different parts of Nigeria due to conflicts and natural disasters, underscoring the importance of reliable record-keeping for the security, integration, and management of migrants (Adewale & Ojo, 2023).

Effective migrant record management underpins government and social service operations. Systems such as the National Identity Number (NIN) and biometric registries provide reliable identification, enabling access to services, promoting security, and supporting governance functions (National Identity Management Commission, 2023). Such records improve healthcare delivery, social welfare distribution, and humanitarian assistance, and enhance state capacity to combat trafficking and irregular migration. However, these technologies depend on ethical data handling and strong institutional safeguards (Okafor & Ozioma, 2022).

While digital identity databases exist in Nigeria, they present ethical and privacy challenges. Individuals must have control over the acquisition, use, and dissemination of personally identifiable information (PII), including biometric identifiers, travel documents, and residence records. Poor governance, lack of ethical awareness, and weak enforcement of privacy regulations have made data breaches, unauthorised access, and misuse increasingly common (Adeleke & Ojo, 2023; Ndukwe, 2022).

Nigeria's information security framework, governed by the NDPA 2023, builds on the Nigeria Data Protection Regulation (NDPR 2019) and the creation of the Nigeria Data Protection Commission (NDPC 2022). Nonetheless, many migration-related agencies, including the Nigeria Immigration Service (NIS), National Identity Management Commission (NIMC), and the National Commission for Refugees, Migrants and Internally Displaced Persons (NCFRMI), often lack the technical expertise, ethics training, and oversight mechanisms needed to comply with these regulations (Adeleke & Ojo, 2023).

Consequently, migrant data may be collected without proper authority, inadequately safeguarded, or shared without explicit consent, increasing the risk of discrimination, stereotyping, surveillance, and identity theft. A notable example occurred in Plateau State in 2022, where a data breach exposed the personal information of over 37,000 individuals, highlighting enforcement gaps (Olaigbe, 2022). Scholars have also raised concerns about biometric nationality, in which politicised identification systems can be manipulated during administrative or electoral processes, undermining migrants' rights (Iwoha & Doeverspeck, 2023).

These challenges illustrate persistent inadequacies in Nigeria's data governance framework. Weak ethical accountability, conflicting institutional priorities, and inconsistent regulations compromise the protection of migrant data. Moreover, the

tension between privacy safeguards and national security often results in state monitoring taking precedence over human rights.

Migrants, particularly those from low-income backgrounds, face heightened risks of marginalisation and abuse, which erodes public trust in government institutions. Without a transparent, human-rights-centred, and ethically sound system for recording migrant data, efforts to modernise migration policy risk exacerbating systemic vulnerabilities.

The prevalence of data breaches, limited compliance culture, and low ethical awareness among migration professionals highlight the urgent need for reform. This study, therefore, seeks to investigate the privacy and ethical challenges of managing migrant records in Nigeria and to propose strategies to enhance data governance, institutional accountability, and the protection of migrants' rights in the digital era.

OBJECTIVES

1. To examine the nature of migrant record management in Nigeria.
2. To identify the ethical challenges encountered in the handling of migrant data.
3. To discuss the existing legal and institutional frameworks governing data privacy in migration management.

MATERIALS AND METHODS

The study employed a narrative review as its method. It was selected because it facilitates a general summary and synthesis of empirical evidence on a particular concept or theme, situating it within the context of current research. A narrative review combines previously published literature on a particular subject, with particular focus on a concept's major ideas, theoretical explanations, methodologies, and findings, as stated by Paré et al. (2015). The literature used in this work focused on a series of core issues: the nature of migrant record management in Nigeria; the ethical challenges encountered in handling migrant data; the application of innovative technologies; the existing legal and institutional frameworks governing data privacy in migration management; and proposed recommendations and future research.

The Nature of Migrant Record Management in Nigeria

Managing migrant records in Nigeria is crucial for effective migration governance and national security, involving the organised collection and use of migrant data for

service provision and policy development (IOM, 2023; Adeleke & Eze, 2022). Key agencies such as the Nigeria Immigration Service (NIS), the National Identity Management Commission (NIMC), and the National Commission for Refugees, Migrants, and Internally Displaced Persons (NCFRMI) maintain separate databases, leading to inefficiencies and gaps in inter-agency coordination (Oloyede & Hassan, 2024; Ibrahim & Musa, 2023).

Despite initiatives like the Migration Information and Data Analysis System (MIDAS) aimed at improving data collection, challenges such as limited funding, technical expertise, and legal gaps persist (Eze, 2022). The data collected includes personal and biometric information, but incompatibilities between digital systems, reliance on paper records in rural areas, and a shortage of skilled personnel increase the risk of mismanagement (Okafor & Ozioma, 2021; Chukwuma & Abubakar, 2023; Adewale & Ojo, 2024). Recent improvements, such as biometric passports and the endorsement of data protection guidelines by the International Organisation for Migration, indicate progress, yet experts emphasise that technology alone cannot address underlying structural and ethical issues; sustainable change requires political will, continuous capacity building, and strong ethical frameworks (Adewale & Ojo, 2024).

Despite efforts to modernise migrant record management in Nigeria, challenges such as weak coordination, technical limitations, and insufficient ethical oversight persist. The findings section below explores these issues, focusing on privacy, unauthorised data use, threats to human rights, lack of ethical awareness, institutional data, and ongoing ethical and security/privacy concerns.

RESULTS

This section presents the key findings of the study on data privacy and ethical challenges in managing migrant records in Nigeria, highlighting systemic and operational issues that compromise privacy and human rights. The analysis revealed six interrelated themes that illustrate the complexities of managing sensitive migration data.

First, concerns about privacy and confidentiality underscore the vulnerability of personal information, including biometric identifiers, travel histories, and medical records, due to weak cybersecurity and limited regulatory enforcement.

Second, unauthorised use and sharing of data reflects coordination gaps among migration agencies, which can result in duplication, misuse, or politically motivated dissemination of migrant information.

Third, threats to human rights emerged as mismanaged data sometimes lead to discrimination, stigmatisation, or the repurposing of humanitarian data for law enforcement.

Fourth, a lack of ethical awareness and institutional accountability highlights deficiencies in training, oversight, and organisational culture that hinder responsible data handling.

Fifth, the findings demonstrate the challenge of balancing ethics, security, and governance, revealing tensions between border security objectives and the protection of migrants' rights.

Finally, ongoing ethical and privacy threats such as breaches, function creep, and political exploitation remain persistent concerns. These findings provide a structured foundation for examining the ethical challenges in migrant record management, which are further explored in the discussion.

DISCUSSION

Ethical Challenges in the Management of Migrant Records

Handling migrant data raises significant ethical concerns regarding privacy, human rights, and security. Such data often include sensitive information, including biometric identifiers, travel history, and medical or family records.

To uphold migrants' dignity, safety, and trust in migration organisations, it is essential that this data is managed ethically. Ethical dilemmas typically arise from the tension between state security objectives and the protection of individual privacy and data rights. While governments may justify extensive data collection for border security, national identity verification, or counter-terrorism purposes, weak ethical standards can lead to misuse or overreach.

1. Concerns about Privacy and Confidentiality

Maintaining privacy and confidentiality is one of the foremost ethical responsibilities in managing migrant data. The digitalisation of migration records, such as through

biometric databases, has made it easier for unauthorised individuals to access sensitive information. In Nigeria, cybersecurity safeguards and data encryption technologies are often inadequate, leaving personal information vulnerable to theft or leakage. Poor infrastructure and limited professional knowledge of data ethics further complicate efforts to protect privacy. Additionally, the Nigeria Data Protection Act (NDPA, 2023) currently lacks robust enforcement mechanisms, thereby exacerbating risks associated with unauthorised access to and misuse of migrant data. Migrants often provide personal information under duress during asylum or deportation processes, limiting genuine consent and contravening ethical principles such as autonomy and informed permission, emphasised in international frameworks like the EU's GDPR (Abebe, 2022; IOM, 2023).

When compared regionally, Kenya and South Africa provide stronger legal safeguards for migrants' data. Kenya's Data Protection Act (2019) establishes a dedicated Data Protection Commissioner with the power to monitor compliance, enforce penalties, and oversee cross-border data transfers, giving individuals greater control over sensitive personal information, including biometric data (Abebe, 2022). Similarly, South Africa's Protection of Personal Information Act (POPIA, 2013) imposes strict processing requirements, purpose limitations, and accountability measures, with a strong emphasis on securing information against misuse and unauthorised disclosure (Abebe, 2022). In contrast, Nigeria's framework is still developing and faces challenges in enforcement, inter-agency coordination, and technical capacity (Eze & Musa, 2023).

2. Unauthorised Use and Sharing of Data

Unauthorised data sharing among government agencies is a persistent ethical challenge. In Nigeria, overlapping roles among the NIS, NIMC, and NPopC often result in duplication of records and inconsistent information-sharing protocols (Okon & Abubakar, 2023). Migrant data may sometimes be repurposed for political profiling or surveillance, raising issues of equity, discrimination, and stigmatisation. By contrast, Kenya and South Africa's regulatory frameworks provide clearer guidance and stronger enforcement mechanisms to prevent unauthorised sharing and ensure accountability (Abebe, 2022).

3. Threats to Human Rights

Mismanaged data can exacerbate discrimination and stigmatisation of migrant populations. In Nigeria, insufficient ethical awareness among officials has led to cases where irregular migrants are incorrectly labelled as security threats, violating

principles of justice, equity, and human dignity (Ojo & Ighodaro, 2023). The stronger institutional oversight in Kenya and South Africa mitigates some of these risks by enforcing legal accountability and providing avenues for redress, ensuring that data handling respects human rights (Abebe, 2022; UNHCR, 2022).

4. Lack of Ethical Awareness and Institutional Accountability

Nigeria continues to face challenges in embedding ethical awareness and institutional accountability across migration agencies. The NDPA (2023) has not been fully implemented, and gaps in training, monitoring, and organisational culture hinder responsible data handling (Oloyede & Nwosu, 2024). Regional examples illustrate the benefits of institutional capacity: Kenya's Data Protection Commission and South Africa's Information Regulator provide structured oversight, ethical guidance, and sanctions for non-compliance, highlighting the importance of strong institutions and training programs in promoting ethical stewardship.

5. Balancing Ethics, Security, and Governance

Ethical management of migrant data requires balancing national security needs with individual privacy rights. While Nigeria prioritises border security and intelligence gathering, inconsistent enforcement of privacy laws undermines ethical compliance (Eze & Musa, 2023). Lessons from Kenya and South Africa suggest that integrating robust legal frameworks, independent oversight, and technical safeguards can achieve a better equilibrium between security and rights protection. International cooperation, such as Nigeria's partnerships with the IOM and the European Union for MIDAS implementation, further strengthens alignment with GDPR standards, though budget and capacity limitations continue to restrict full compliance (UNHCR, 2022; IOM, 2023).

6. Ongoing Ethical and Privacy Threats in Migrant Data Management

Persistent challenges such as data breaches, "function creep" of biometric systems, and politicisation of identification processes remain critical. A 2022 breach in Plateau State exposed over 37,000 individuals' records, illustrating weaknesses in enforcement and infrastructure (Iwuoha & Doeverspeck, 2023). While Kenya and South Africa have robust regulatory authorities to respond to breaches and protect migrant privacy, Nigeria's enforcement remains uneven, underscoring the urgent need for technical capacity-building, inter-agency collaboration, and rights-based, ethical governance.

Existing Legal and Institutional Frameworks for Data Privacy in Migration Management

The safeguarding of personal data in migration management has become a significant issue in both international and national government. Migration systems manage vast quantities of sensitive information, including biometrics, demographic data, and personal identifiers, hence requiring well-defined legal and institutional frameworks to protect privacy and guarantee ethical adherence. The development of data protection laws in Nigeria has sped up in the last few years. For example, the Nigeria Data Protection Act (NDPA) 2023 sets the legal framework for keeping an eye on data processing in several areas, such as migration. Oloyede and Nwosu (2024) note that execution is still not uniform, and that migration institutions do not work together very well.

1. The Legal Status in Different Parts of the World and in Different Areas

International human rights norms and regional legal instruments play a crucial role in regulating data privacy and protection in the context of global mobility. Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights affirm the right to privacy and protect against arbitrary intrusion. The UNHCR (2022) states that these principles serve as the moral foundation for the global management of migrant data.

The General Data Protection Regulation (GDPR) of the European Union has set a global benchmark for data privacy, emphasising legality, fairness, transparency, purpose limitation, and data minimisation (European Data Protection Board, 2021). Many African nations have adopted similar principles, exemplified by the African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention), which became effective in 2019 as the first continent-wide framework for personal data protection. Abebe (2023) notes that this convention encourages member states to develop their own legislation regarding data collection, handling, and sharing. These principles assist data controllers, including immigration authorities, humanitarian organisations, and border agencies.

2. The National Legal System: The Nigerian Data Protection Act (NDPA) of 2023

The Nigeria Data Protection Act (NDPA), enacted in 2023, serves as the primary legislation for privacy protection in Nigeria, establishing the Nigeria Data Protection Commission (NDPC) as the enforcement body.

Oloyede and Hassan (2024) argue that the NDPA represents a significant advancement over the Nigeria Data Protection Regulation (NDPR) of 2019 by incorporating principles such as lawful processing, consent, purpose limitation, data minimisation, and data subject rights, aligning with global best practices.

The Act is particularly crucial for migration management, as it applies to organisations like the Nigeria Immigration Service (NIS), the National Identity Management Commission (NIMC), and the National Commission for Refugees, Migrants, and Internally Displaced Persons (NCFRMI). Okonkwo and Ajayi (2023) emphasise that these agencies are now legally required to ensure the transparent, secure, and lawful handling of migrant data. However, challenges remain in enforcement, as Chukwuma and Hassan (2024) argue that many public entities lack internal data protection officers and compliance frameworks, which hinder effective implementation.

3. Institutional Structures for Data Privacy in Migration Management

In Nigeria, several important institutions oversee migration data, but their roles often overlap. The Nigeria Data Protection Commission (NDPC) ensures that the NDPA 2023 is followed, sets out rules for doing so, and punishes those who violate them (NDPC 2024).

The Nigeria Immigration Service (NIS) works with the International Organisation for Migration (IOM) to manage biometric and travel data. One way they do this is through the Migration Information and Data Analysis System (MIDAS) (IOM 2023).

The National Identity Management Commission (NIMC) oversees the National Identity Database (NIDB) and issues the National Identification Number (NIN), which is sometimes used to verify people's identities when they move (Eze & Musa 2023).

The National Commission for Refugees, Migrants, and Internally Displaced Persons (NCFRMI) gathers information about migration and humanitarian needs while protecting the rights of at-risk groups. Still, there are coordination problems. Ibrahim and Musa (2023) argue that poor data-sharing rules and overlapping institutions make it harder to comply with them. The NDPC's supervision is further hindered by limited resources and a complex bureaucracy.

4. Nigeria's Data Privacy Framework Has Legal and Policy Holes

The NDPA 2023 has some operational and policy issues, despite some good points. Oloyede and Nwosu (2024) contend that penalties for breaches of privacy are feeble

and enforced inconsistently. The NDPA does not require Data Protection Impact Assessments (DPIAs) for high-risk data operations, unlike the GDPR. This is an important difference in cases involving biometrics. Asogwa and Nwafor (2022) emphasise the lack of explicit inter-agency data exchange regulations, resulting in unregulated data transfers. The NDPA similarly lacks definitive guidelines for cross-border data flows, despite Nigeria's collaboration with organisations like the IOM and the EU on migration data initiatives. Ajayi and Okonkwo (2022) assert that Nigeria's data protection strategy emphasises technical compliance at the expense of moral accountability, advocating for the integration of ethical principles such as fairness, respect, and transparency into the culture of data governance.

5. Different Points of View and Working Together with Other Countries

When comparing Nigeria, Kenya, and South Africa, clear differences emerge in the legal and institutional frameworks governing the protection of migrant data. Nigeria's Nigeria Data Protection Act (NDPA, 2023), building on the Nigeria Data Protection Regulation (NDPR, 2019) and the establishment of the Nigeria Data Protection Commission (NDPC, 2022), provides a foundational framework for safeguarding personal information, including that of migrants. The Act addresses principles such as lawful processing, consent, purpose limitation, and data minimisation. However, enforcement remains inconsistent, partly due to limited technical capacity, budget constraints, and fragmented inter-agency coordination among the Nigeria Immigration Service (NIS), National Identity Management Commission (NIMC), and National Commission for Refugees, Migrants, and Internally Displaced Persons (NCFRMI) (Eze & Musa, 2023).

Kenya's Data Protection Act (2019), in contrast, offers a more robust and detailed legal framework. It establishes the Office of the Data Protection Commissioner as a dedicated regulatory authority with strong powers to monitor compliance, enforce penalties, and oversee cross-border data transfers. The Act explicitly addresses sensitive personal data, including biometric identifiers, and emphasises individuals' rights to access, correct, and control their personal information. For migration data, this provides a clearer mechanism for protecting vulnerable populations and ensures accountability in data handling (Abebe, 2022).

South Africa's Protection of Personal Information Act (POPIA, 2013) similarly sets high standards for privacy protection, including strict requirements for processing personal data, obtaining consent, and securing information. POPIA applies to both public and private institutions, requiring organisations to implement comprehensive

information security measures and to report breaches to regulators. For migrant records, POPIA's emphasis on purpose limitation and accountability provides strong ethical and legal safeguards against misuse or unauthorised disclosure (Abebe, 2022).

In comparison, Nigeria has made progress by adopting principles similar to those in Kenya and South Africa and aligning its systems with international standards, such as the EU's GDPR through partnerships with the International Organisation for Migration (IOM, 2023) and the European Union's support for the Migration Information and Data Analysis System (MIDAS) (UNHCR, 2022). However, practical challenges such as weak enforcement, insufficient training, and inter-agency overlap mean that Nigeria still lags behind its regional peers in translating legal provisions into effective protection for migrants. These contrasts highlight the importance of continuous institutional strengthening, international cooperation, and a rights-based approach to data governance to ensure that ethical and privacy principles are consistently upheld across migration management systems.

6. Making Legal and Institutional Structures Stronger

For Nigeria to improve its current processes, it needs to focus on making the law more consistent, working together with other agencies, and enforcing the law. Chukwuma and Hassan (2024) say that migration agencies should set up special data protection teams and do frequent audits. Parliamentary and judicial supervision might help NDPC do its job of regulating. Oloyede and Hassan (2024) also support that migration databases should have DPIAs, that cross-border data exchange should be regulated, and that privacy-by-design should be built into digital platforms. Training and efforts to raise public awareness would also help create a stronger culture of data protection and hold institutions accountable.

CONCLUSION

The management of migrant records in Nigeria has seen significant transformation through the adoption of digital technologies, including biometric registration, national identity databases, and electronic migration systems. These innovations have enhanced the efficiency of data collection, verification, and service delivery. However, they have also introduced complex ethical and privacy challenges that require urgent attention. This study finds that migrant data is frequently collected without proper consent, stored in vulnerable systems, and shared across institutions without adequate authorisation. Such practices expose migrants to identity theft, misuse of personal information, and violations of fundamental rights. The tension between national

security objectives and the protection of individual privacy further complicates the governance of migration data. The ethical and privacy challenges stem largely from systemic deficiencies, including weak inter-agency collaboration, limited technical infrastructure, insufficient institutional capacity, and inadequate enforcement of data protection laws. While recent reforms, such as the Nigeria Data Protection Act (2023) and the establishment of the Nigeria Data Protection Commission (NDPC) represent a positive step, much remains to be done to ensure compliance, accountability, and public confidence.

To achieve a sustainable and ethically sound framework, Nigeria must adopt a rights-based, transparent, and secure approach to migrant data management. Strengthening institutional capacity, enhancing inter-agency coordination, integrating ethical principles into operational culture, and investing in cybersecurity are essential. Furthermore, aligning practices with international and regional standards and collaborating with organisations such as IOM, UNHCR, and ECOWAS can provide technical expertise, policy harmonisation, and cross-border learning. Ultimately, a balanced approach that safeguards migrants' privacy and dignity while meeting legitimate national security objectives is crucial for effective and responsible migration governance.

RECOMMENDATION

1. **Harmonisation of Legal Frameworks:** The Nigerian government should consolidate existing data protection instruments by integrating the Nigeria Data Protection Regulation (NDPR, 2019), the Nigeria Data Protection Commission (NDPC, 2022), and the Nigeria Data Protection Act (NDPA, 2023) into a unified and enforceable regulatory framework for migration data management. This consolidated framework should clearly define standards for ethical data handling, informed consent, cross-border data sharing, and strict penalties for violations. Aligning Nigeria's legal framework with international standards, such as the EU's GDPR and the African Union Malabo Convention, can improve accountability, eliminate overlaps, and strengthen compliance across migration-related institutions.
2. **Strengthening Institutional Capacity and Infrastructure:** Migration-related institutions, including the Nigeria Immigration Service (NIS), the National Identity Management Commission (NIMC), and the National Commission for Refugees, Migrants, and Internally Displaced Persons (NCFRMI), should be adequately resourced and equipped with modern infrastructure to ensure secure and

efficient data management. A centralised, interoperable data-sharing platform with robust access controls should be established to reduce duplication and unauthorised access. Regular professional training on data ethics, privacy protection, and cybersecurity should be mandatory to cultivate a culture of responsibility and ethical compliance.

3. **Embedding Ethical Standards in Operational Culture:** Ethical principles should be fully integrated into the core operations of all institutions handling migrant data. Developing a comprehensive professional code of conduct, coupled with periodic audits and clearly defined disciplinary measures, can enhance transparency and accountability. Establishing ethical review boards or committees will ensure that data management practices consistently respect the rights and dignity of migrants. Comparative lessons from South Africa and EU member states show that independent ethics oversight can significantly improve adherence to privacy and human-rights standards.

4. **Investment in Cybersecurity and Data Risk Management:** Continuous investment in cybersecurity systems, encryption technologies, and data risk management tools is essential to safeguard sensitive migrant information. Regular independent security audits should identify and address system vulnerabilities, while robust data recovery and incident response mechanisms will mitigate breaches and unauthorised disclosures. Learning from global best practices, including the EU and UNHCR guidelines, Nigeria can develop proactive systems that balance efficiency with data protection.

5. **Rights-Based Data Governance:** Management of migrant data should prioritise human rights, privacy, and informed consent. A rights-based approach ensures that technological efficiency does not override ethical responsibility. Nigeria should align its migration data practices with international standards and conventions that emphasise fairness, transparency, and protection for vulnerable populations, thereby building public trust and upholding human dignity.

6. **International and Regional Collaboration:** Nigeria should deepen partnerships with international and regional organisations such as the International Organisation for Migration (IOM), the United Nations High Commissioner for Refugees (UNHCR), and the Economic Community of West African States (ECOWAS). These collaborations can strengthen technical expertise, support policy harmonisation, and enable cross-border capacity building. Engagement with civil

society organisations and research institutions will further facilitate oversight, advocacy, and shared learning, promoting globally informed ethical governance practices.

7. **Public Awareness and Accountability:** Public education is crucial for reinforcing data protection and accountability. Migrants and the public should be well informed about their privacy rights, the purpose of data collection, and available redress mechanisms in cases of misuse. Government agencies should publish regular reports on data management practices to promote transparency and trust. A participatory approach, informed by both local realities and international standards, will foster confidence in Nigeria's migration governance and encourage compliance with ethical data standards.

CONFLICT OF INTEREST DECLARATION

We, Ailakhu, Ugonna Vivian and Ambrose, Eromosele Smart (authors), clearly declare that there is no conflict of interest in the study/paper titled: Data Privacy and Ethical Challenges in the Management of Migrant Records in Nigeria.

REFERENCES

- Abebe, T. (2023). Data privacy and human rights in migration management. *Journal of Migration Studies*, 14(2), 45–61.
- Adeleke, O. & Ojo, A. (2023). Data protection and migration management in Nigeria: Challenges and prospects. *Journal of African Policy Studies*, 7(2), 112–130.
- Adeleke, O. (2022). Proportionality and ethical decision-making in data governance. *Information Ethics Review*, 6(3), 75–90.
- Adewale, T. & Ojo, A. (2023). Migrant record-keeping and governance challenges in Nigeria. *African Journal of Public Administration*, 12(1), 22–39.
- Adewale, T. & Ojo, A. (2024). Ethical issues in digital migration databases in West Africa. *International Journal of Information Management*, 59, 102512.
- Adeyemi, K. & Olaniyan, S. (2021). Data ethics in public administration: Lessons from Nigeria. *Nigerian Journal of Administrative Studies*, 18(1), 11–28.
- Ajayi, L. & Okonkwo, M. (2022). Nigeria's data protection framework: Technical compliance versus ethical accountability. *African Journal of Cybersecurity and Policy*, 3(1), 34–50.
- Asogwa, F. & Nwafor, C. (2022). Inter-agency data sharing and privacy challenges in migration governance. *Journal of Information Policy*, 12, 55–72.
- Asogwa, F. & Ozioma, U. (2021). Unauthorised data sharing and migrants' right to informational self-determination. *Nigerian Journal of Human Rights*, 9(2), 44–59.
- Chukwuma, I. & Abubakar, H. (2023). Digital migration records and operational inefficiencies in Nigeria. *African Journal of Information Science*, 15(1), 88–102.
- Chukwuma, I. & Hassan, A. (2024). Migration governance and ethical data management in Nigeria. *International Journal of African Governance*, 11(1), 1–19.
- Dentons. (2022). *Global data protection laws: Nigeria overview*. Dentons Legal Insights. <https://www.dentons.com/en/insights>

- European Data Protection Board. (2021). Guidelines on the implementation of the GDPR. <https://edpb.europa.eu/>
- Eze, N. & Musa, T. (2023). Balancing security and ethics in migrant data management: Nigeria case study. *Journal of African Security Studies*, 8(2), 101–120.
- Eze, N. (2022). Migration information and data analysis system (MIDAS) in Nigeria: Opportunities and limitations. *African Journal of Technology and Governance*, 4(2), 33–47.
- Gonzalez, L. & Staddon, J. (2021). Data minimisation and ethical governance in information systems. *Information Systems Ethics Journal*, 7(1), 15–30.
- Government of Kenya. (2019). *Kenya Data Protection Act, No. 24 of 2019*. Nairobi, Kenya: National Council for Law Reporting. <https://www.dataprotection.go.ke>
- Government of South Africa. (2013). *Protection of Personal Information Act 4 of 2013(POPIA)*. Pretoria, South Africa: Government Printer. <https://www.justice.gov.za>
- Ibrahim, S. & Musa, T. (2023). Institutional coordination and data sharing in Nigerian migration governance. *Nigerian Journal of Public Administration*, 17(3), 87–102.
- Ibrahim, S. (2023). Dual use of humanitarian data and ethical implications. *Migration Ethics Review*, 5(1), 50–68.
- International Organisation for Migration (IOM). (2023). *Migration data and ethical standards: Do no harm guidance*. Geneva: IOM.
- International Organisation for Migration (IOM). (2025). *Migration trends in West Africa: Labour, commerce, and displacement*. Geneva: IOM.
- Iwuoha, V. & Doevenspeck, M. (2023). Biometric nationality and political exploitation in Nigeria. *African Journal of Migration Studies*, 11(1), 44–63.
- Johnson, R. (2020). *Principles of data privacy and ethics in information management*. Oxford University Press.
- National Identity Management Commission (NIMC). (2023). *Annual report on National Identity Number (NIN) enrolment and biometric systems*. Abuja, Nigeria: NIMC.

- Ndukwe, C. (2022). Ethical handling of personal data in Nigeria: Challenges and prospects. *Nigerian Journal of Information Ethics*, 5(2), 25–41.
- Nigeria Data Protection Commission (NDPC). (2023). *Guidelines for implementing the Nigeria Data Protection Act 2023*. Abuja, Nigeria: NDPC.
- Okafor, I. & Ozioma, U. (2022). Ethical management of digital identity databases: Nigeria experience. *African Journal of Digital Governance*, 5(1), 12–28.
- Okafor, I. & Ozioma, U. (2021). Challenges of managing biometric and digital migration records in Nigeria. *Journal of African Information Systems*, 13(2), 45–60.
- Okonkwo, M. & Ajayi, L. (2023). Legal compliance and gaps in Nigerian migration data management. *African Journal of Law and Technology*, 9(2), 60–78.
- Olaigbe, O. (2022). Data breaches and privacy violations in Plateau State health agency. *Nigerian Journal of Cybersecurity*, 6(1), 77–89.
- Oloyede, F. & Hassan, A. (2024). Institutional accountability in Nigerian migration data governance. *Journal of African Public Administration*, 16(1), 33–51.
- Oloyede, F. & Nwosu, P. (2024). Ethical gaps in data handling and sharing in migration institutions. *Nigerian Journal of Information Ethics*, 7(1), 15–30.
- Paré, G., Trudel, M.-C., Jaana, M., & Kitsiou, S. (2015). Synthesising information systems knowledge: A typology of literature reviews. *Information & Management*, 52(2), 183–199. <https://doi.org/10.1016/j.im.2014.08.008>
- Paul, M. (2024). *Global perspectives on data protection and ethical governance*. Cambridge University Press.
- UNHCR. (2022). *Guidelines for data protection in migration and humanitarian operations*. Geneva: United Nations High Commissioner for Refugees.
- Voigt, P. & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer.