Voter Privacy and Umpires' Transparency: An Assessment of The Electoral Bodies' Compliance With The Nigeria Data Protection Act (NDPA) 2023

A Documentary Assessment of Voter Privacy and Data Transparency Compliance by Electoral Bodies in Nigeria.

Olumide Babalola, PhD
Solomon Okedara, Esq.

Digital Rights Lawyers Initiative

Luminate



The Digital Rights Lawyers Initiative (DRLI) is a Nigerian civil society organisation committed to promoting and protecting digital rights, privacy, data protection, freedom of expression and access to justice. DRLI works at the intersection of law, technology and human rights through legal advocacy, strategic litigation, research, policy engagement, public education and stakeholder collaboration. The organisation seeks to strengthen legal and institutional safeguards for individuals and communities while promoting responsible governance of personal data and emerging technologies in Nigeria and beyond.

Copyright and Use
© 2026 Digital Rights Lawyers Initiative (DRLI). All rights reserved. This publication may be reproduced, cited or otherwise used for non-commercial research, educational, advocacy and public-interest purposes, provided that appropriate acknowledgement is given to the Digital Rights Lawyers Initiative and the title of the publication is clearly cited. No part of this publication may be reproduced, adapted, distributed or commercially exploited without the prior written permission of DRLI, except as permitted by applicable law.

Authors:
Olumide Babalola, PhD & Solomon Okedara, Esq.

DIGITAL RIGHTS LAWYERS INITIATIVE (DRLI)
Aggey House (6th Floor)
12 Berkeley Street, Off KingGeorge Road
Onikan, Lagos, Nigeria
olumide.b@digitalrightslawyers.org, s.o@digitalrightslawyers.org, and solomon.o@digitalrightslawyers.org .
Website: www.digitalrightslawyers.org

AUTHORS' PROFILE PAGE

OLUMIDE BABALOLA, PHD

Olumide Babalola, PhD is a Nigerian legal scholar, privacy and data protection lawyer, author and digital rights advocate. He is the Managing Partner of Olumide Babalola LP and a leading practitioner and researcher in privacy, data protection, digital rights and technology law. He holds an LLM in International Commercial Law with ICT & Commerce from the University of Reading, United Kingdom, and completed his doctoral research at the University of Portsmouth, United Kingdom, where his research focused on the development of the constitutional right to privacy in Nigeria through the courts. His doctoral thesis examines Nigerian privacy jurisprudence comparatively with developments in South Africa and Kenya.

Dr Babalola has combined legal practice with teaching and academic research in the United Kingdom and Nigeria. He previously served as a Teaching Assistant in Law at the University of Manchester and taught law at the University of Portsmouth. He has also taught at Lead City University, Ibadan, where he has served as an adjunct lecturer, and currently serves as a Lecturer at Caleb University, Lagos. His academic engagement has focused particularly on privacy law, data protection, technology law and digital rights. He is the author of several books and scholarly works on privacy and data protection, including Casebook on Data Protection, Privacy and Data Protection Law in Nigeria, Digital Rights in Nigeria: Through the Cases, Emerging Jurisprudence on Privacy and Data Protection in Nigeria, and Annotated Nigeria Data Protection Act 2023. His scholarly publications include 'Nigeria's Data Protection Legal and Institutional Model: An Overview' in the International Data Privacy Law, 'The Constitutional Origins of the Right to Privacy in Nigeria' in the African Journal on Privacy & Data Protection. His research and scholarship have contributed significantly to the development of privacy and data protection discourse in Nigeria.

Dr Babalola has also been involved in significant privacy and data protection litigation and advocacy in Nigeria, including the landmark Digital Rights Lawyers Initiative v National Identity Management Commission (2021) LPELR-55623(CA), which addressed the relationship between data protection and the constitutional right to privacy. He is the pioneer Chair of the Nigerian Bar Association Data Protection Committee and has served in professional and international privacy and data-governance networks. He is also the founder of the Data Privacy Lawyers Association of Nigeria (DPLAN) and co-founder of Digital Rights Lawyers Initiative.

SOLOMON OKEDARA, ESQ.

Solomon Okedara is a Nigerian digital rights lawyer, researcher and consultant whose nearly two decades of legal practice, scholarly inquiry and strategic intervention have placed him at the forefront of Nigeria's evolving digital rights landscape. His work sits at the critical intersection of law, technology, human rights and democratic governance. As a consultant, Solomon has advised governments, private organisations and multilateral institutions on data protection, privacy, digital identity, technology regulation and broader digital rights issues. His portfolio includes supporting the European Investment Bank (EIB) on the human rights assessment of Nigeria's Digital Identity Project, examining the privacy, data protection and human rights implications of a population-scale digital identity system linked to international development financing of Nigeria's digital identity (e-ID) project.

His professional accomplishments extend beyond advisory practice into landmark public-interest litigation and institutional accountability. Solomon has been instrumental in advancing Nigerian jurisprudence on digital rights, including the recognition of privacy as encompassing personal data protection in the context of digital identity, challenges to repressive provisions of the Cybercrimes Act, and strategic interventions before the ECOWAS Court to strengthen freedom of expression and media freedom. His litigation record reflects a sustained commitment to ensuring that public authorities and corporate institutions exercise power within the boundaries of constitutional rights, lawful regulation and democratic accountability.

Since 2018, Solomon has served as a Legal Researcher with Columbia University's Global Freedom of Expression, contributing legal research, high-quality case analyses and scholarly commentary on freedom of expression jurisprudence across more than 120 jurisdictions. This engagement has deepened his comparative understanding of constitutional rights, international human rights standards and the evolving relationship between law, technology and democratic institutions. In 2025, he was awarded a Data Governance in Africa Research Fund grant, leading research into the unequal enforcement of Nigeria's data protection laws and its implications for effective data governance. The research examined regulatory fragmentation, institutional accountability and the differential treatment of public and private data controllers, contributing to wider conversations on the credibility, fairness and effectiveness of data protection enforcement in Africa.

Solomon's authority to engage on voters' privacy and electoral accountability is exemplified by his pioneering litigation in Solomon Okedara v. Independent National Electoral Commission: FHC/ABJ/CS/1007/2023, instituted immediately after the 2023 General Election. The case interrogates INEC's obligation to conduct a Data Protection Impact Assessment (DPIA) in processing voters' personal data, advancing a consequential legal and institutional intervention aimed at pushing Nigeria's electoral management body towards greater transparency, accountability and public trust. By placing voters' privacy and personal data protection at the heart of electoral integrity, Solomon's work challenges the notion that credible elections are measured solely by the conduct and outcome of voting, rather than also by the protection of the rights of those whose data sustains the electoral system. As a co-author of this work, Solomon brings not only scholarly depth and extensive digital rights expertise, but also first-hand experience in deploying legal mechanisms to advance a more privacy-respecting, trustworthy and democratically accountable electoral process.

DISCLAIMER

Every reasonable effort has been made by the Digital Rights Lawyers Initiative (DRLI) and the authors to ensure the accuracy, reliability and completeness of the information, analysis and references contained in this report. The report has been prepared based on legislation, regulations, official publications, institutional documents, publicly available information, responses to requests for information, academic literature and other materials considered relevant to the subject of the study.

The information and legal position presented in this report reflect the position reasonably ascertainable at the time of the research and were believed to be accurate as of 15th September 2026. However, laws, regulations, institutional policies, electoral practices, official websites and other relevant information may change after the date of publication. Accordingly, the report should not be understood as providing a guarantee that all information will remain current or applicable after that date.

This report is intended for research, educational, advocacy, policy and public-interest purposes. It is not intended to constitute legal advice, nor should any part of it be relied upon as a substitute for obtaining professional legal, regulatory or other appropriate advice in relation to a particular matter or circumstance. Readers are encouraged to consult the relevant legislation, regulations, official documents and competent authorities where decisions are to be made on the basis of the information contained in this report.

While DRLI has taken reasonable steps to verify the information relied upon, the report may contain information obtained from third parties, public institutions, official websites and other external sources. DRLI does not independently warrant the continued accuracy, completeness or availability of information originating from such sources. The inclusion of any institution, practice, policy, statement or source in this report should not, without more, be construed as an endorsement, finding of wrongdoing or definitive determination of legal compliance or non-compliance, except where expressly stated and supported by the evidence presented.

DRLI accepts no responsibility or liability for any loss, damage, claim or other consequence arising from the use, interpretation or application of the information, analysis, findings or recommendations contained in this report, particularly where the contents are used for purposes or in contexts different from those for which the report was prepared. The findings and recommendations should be considered in light of the methodology, scope, limitations and evidentiary basis set out in the report.

The views, interpretations, findings and recommendations expressed in this report are those of the authors and DRLI and do not necessarily reflect the views of any institution, agency, expert reviewer, contributor or funding partner acknowledged in the report.

ACKNOWLEDGEMENTS

The **Digital Rights Lawyers Initiative** (DRLI) gratefully acknowledges the experts who generously gave their time to review earlier drafts of this study.

We are particularly grateful to: **Prof. Abiodun Odusote ACIS** (Professor of Public Law, University of Lagos); **Dr Efe Lawrence-Ogeide** (Associate Partner, Ranbrook Partners LP); **Uchenna Nnawuchi PhD, FCIArb (UK),** University of Sheffield, UK; **Mubarak Raji** (Privacy and AI governance Doctoral Researcher at the School of Information Sciences, University of Illinois at Urbana-Champaign) and **Dr Jerome Uchenna Orji** (Cybersecurity law expert), for their careful review of the draft and for the valuable comments, critical observations and constructive recommendations they provided. Their expertise and perspectives contributed significantly to strengthening the study's legal analysis, methodology, assessment and policy recommendations.

We also express our sincere appreciation to the **Nigeria Data Protection Commission (NDPC)** for its cooperation and for responding to the Freedom of Information requests made in the course of this study. We equally appreciate the other public institutions and agencies that responded to our enquiries and provided information that assisted the research team in developing and validating the evidence base for this study. Their responses and cooperation contributed to a more informed assessment of the state of voter privacy and data transparency within Nigeria's electoral process.

We also gratefully acknowledge the members of our research and project team who contributed to the conceptualisation, research, data collection, analysis, review and production of this study. We particularly appreciate the leadership and coordination of **Solomon Etisang, Esq**., whose direction and commitment were instrumental to the completion of the project. We further recognise the contributions of all members of the DRLI team whose collective efforts, diligence and expertise helped bring this study to completion.

Finally, we gratefully acknowledge **Luminate** for its financial support towards this project. The funding provided the resources necessary to undertake the research, data collection, analysis and production of this study. We appreciate the Funder's support for research and initiatives that contribute to strengthening voter privacy, data protection, transparency and accountability within Nigeria's electoral process.

The authors are grateful for the intellectual engagement and rigorous scrutiny provided by all the reviewers. Acknowledgement of their contributions does not imply that they endorse the findings, conclusions or recommendations of this study. Responsibility for the analysis, interpretations, findings and recommendations contained in the final report rests solely with the authors and the Digital Rights Lawyers Initiative.

LIST OF ABBREVIATIONS AND ACRONYMS

Abbreviation/ Acronym	Meaning
BVAS	Bimodal Voter Accreditation System
CAR	Compliance Audit Return
CSO	Civil Society Organisation
DPA	Data Processing Agreement
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DRLI	Digital Rights Lawyers Initiative
EC8A	Polling Unit Result Form
EMB	Electoral Management Body
FOSIECON	Forum of State Independent Electoral Commissions of Nigeria
FOI	Freedom of Information
GAID	General Application and Implementation Directive
ICT	Information and Communication Technology
INEC	Independent National Electoral Commission
IReV	INEC Result Viewing Portal
NDPA	Nigeria Data Protection Act
NDPC	Nigeria Data Protection Commission
NDPR	Nigeria Data Protection Regulation
NGO	Non-Governmental Organisation
OSCOLA	Oxford Standard for the Citation of Legal Authorities
PII	Personally Identifiable Information
RBAC	Role-Based Access Control
ROPA	Record of Processing Activities
SIEC	State Independent Electoral Commission
SIECs	State Independent Electoral Commissions
SMS	Short Message Service
URL	Uniform Resource Locator
WHO	World Health Organization


YOU ARE WELCOME

TABLE OF CONTENTS

Acknowledgements	5
List of Abbreviations and Acronyms	6
Executive Summary	10
Definition of Terms	11
CHAPTER ONE	**14**
Introduction	**14**
1.1 Background to the Study	15
1.2 Electoral Governance and Personal Data Processing in Nigeria	15
1.3 Emergence of Data Protection Regulation in Nigeria	16
1.4 Statement of the Problem	17
1.5 Objectives of the Study	18
1.6 Scope and Limitations	18
1.7 Methodology and Sources of Data	19
CHAPTER TWO	**21**
Electoral Bodies and Data Processing Operations in Nigeria	21
2.1 Structure and Mandate of the Independent National Electoral Commission (INEC)	22
2.1.1 Constitution and Statutory Mandate	22
2.1.2 INEC as a Data Controller of Major Importance	22
2.1.3 Financial and Operational Autonomy under the Electoral Act 2026	22
2.2 Structure and Mandate of State Independent Electoral Commissions (SIECs)	23
2.2.1 Constitutional Foundation	23
2.2.2 SIECs as Data Controllers	23
2.2.3 Operational Challenges and Capacity Constraints	23
2.3 Categories of Personal Data Processed by Electoral Bodies	23
2.3.1 General Personal Data	23
2.3.2 Sensitive Personal Data (Biometric Data)	23
2.3.3 Special Consideration for Sensitive Data Processing	24
2.4 Voter Registration and Biometric Data Collection	24
2.4.1 The Voter Registration Process	24
2.4.2 Legal Framework for Biometric Data Processing	24
2.4.3 Consent and Transparency Concerns	24
2.4.4 Data Privacy Impact Assessment (DPIA) Requirement	25
2.5 Digital Election Infrastructure and Data Ecosystems	25
2.5.1 Overview of Digital Election Systems	25
2.5.2 The Bimodal Voter Accreditation System (BVAS)	26
2.5.3 Data Flow in BVAS Operations	26
2.5.4 INEC Result Viewing Portal (IRev)	28
2.5.5 Data Protection Implications of IRev	28
2.5.6 The National Voter Register	28
2.5.7 Security Requirements for the Voter Register	29
2.6 Third-Party Data Sharing and Technology Vendors	29
2.6.1 The Data Processing Ecosystem	29

2.6.2 Categories of Third-Party Processors	29
2.6.3 Data Processor Obligations Under the NDPA	30
2.6.4 NDPC-INEC Partnership and Vendor Accountability	30
CHAPTER THREE	**32**
Assessment of Compliance with the NDPA 2023	**32**
3.1 Transparency and Privacy Notice Compliance	33
3.1.1 Legal Framework for Transparency	33
3.1.2 The Findings: Widespread Non-Compliance	33
3.1.3 INEC's Website Non-Compliance	33
3.1.4 States' Independent Electoral Commissions' Compliance	35
a. Transparency Implication	36
3.2 Filing of Annual Data Protection Compliance Audit Returns	38
3.2.1 Legal Framework	38
3.2.2 The Findings	38
3.2.3 Assessment of Compliance Level	38
3.2.4 Data Breach Reporting and Incident Response Mechanisms	38
3.2.4.1 Legal Framework	38
3.2.4.2 The Emeka Ike Breach: Reporting Compliance Analysis	39
3.2.4.3 Analysis of Compliance with Section 40 Obligations	39
3.2.4.4 Implications and Broader Conclusions	40
CHAPTER FOUR	**41**
Policy Recommendations	**41**
4.1 Legislative and Regulatory Reforms	42
4.2 Strengthening NDPC Oversight of Electoral Bodies	42
4.3 Institutionalisation of Privacy Governance Frameworks	43
4.4 Mandatory DPIAs for Electoral Technologies	45
4.5 Standardisation of Privacy Notices and Consent Practices	45
4.6 Improvement of Data Subject Rights Response Mechanisms	46
4.7 Capacity Building and Training for Electoral Officials	47
4.8 Public Awareness and Voter Education on Data Rights	48
CHAPTER FIVE	**50**
Conclusion	**50**
5.1 Summary of Findings	51
5.2 Implications for Democratic Governance and Electoral Integrity	51
5.3 Final Reflections	52

EXECUTIVE SUMMARY

Background and Problem

Nigeria's electoral system now runs on a massive bedrock of personal data. The Independent National Electoral Commission (INEC) collects and retains biometric and demographic records for more than 94 million registered voters, while 36 State Independent Electoral Commissions (SIECs) process comparable personal data at the subnational level. This data is central to constitutionally protected voting and privacy rights of citizens, yet its collection and use through systems such as the Bimodal Voter Accreditation System (BVAS), the INEC Result Viewing Portal (IReV), and the Continuous Voter Registration process create an unresolved tension between electoral transparency and the privacy guarantees of the Nigeria Data Protection Act (NDPA) 2023. Recent incidents (including a voter-data breach affecting an individual voter, allegations of unauthorised use of voter data in a senatorial recall attempt, and a dispute over INEC's fee for public access to the voter register) signal that these tensions are not merely theoretical.

Purpose and Approach

This study assesses how well INEC and the SIECs comply with the NDPA's transparency and accountability obligations and its General Application and Implementation Directive (GAID). It examines the categories of personal data these bodies collect, the digital infrastructure through which that data moves, and the legal basis for its processing, aiming to propose a balanced framework and evidence-based reforms. The analysis combines a doctrinal review of the NDPA, the Electoral Act 2026, and relevant case law with a compliance audit: a website-based, five-indicator transparency assessment applied to INEC and all 36 SIECs, and a detailed case study of INEC's handling of the 2026 "Emeka Ike" voter-data breach against the three statutory obligations in Section 40 of the NDPA.

Key Findings

- INEC, despite its status as a data controller of major importance, operated without any privacy policy on its website until compelled by litigation; the policy it eventually published addresses only incidental matters such as cookies and recruitment, and is silent on its core activities of biometric capture, BVAS, and IReV. INEC has also not published Data Protection Officer contact details, contrary to the GAID.
- All 36 SIECs assessed show a near-total absence of privacy governance: most lack an independent website, and none was found to have a published privacy policy, leaving voters at the subnational level with materially weaker protection than those interacting with INEC.
- No public evidence exists of any current NDPC compliance audit, return filing, or enforcement action involving INEC, the SIECs, or political parties, despite these bodies controlling the country's largest citizen database.
- INEC's response to the Emeka Ike breach fell short on every limb of Section 40: acknowledgment followed public exposure rather than preceding it, no confirmation of timely NDPC notification was made public, the affected individual was not directly notified, and no breach documentation was disclosed.
- A recurring pattern emerges across these findings: compliance steps taken by electoral bodies have generally followed litigation, public pressure, or breach exposure, rather than proactive institutional design.

Implications

These gaps carry consequences beyond technical non-compliance. They risk eroding public trust in the integrity of the electoral process, create a geographic disparity in privacy protection between federal and state levels, leave the lawful basis for mandatory biometric collection insufficiently communicated to voters, and suggest an implicit hierarchy of accountability in which powerful public institutions face limited enforcement. With Nigeria approaching the 2027 general elections, the credibility of the process will depend not only on the accuracy and security of voter data systems, but on whether citizens can trust that their biometric and personal information is handled lawfully and transparently.

Recommendations

The study proposes a coherent reform programme organised around three pillars:

- Legislative and regulatory reform, including a sector-specific Electoral Data Protection Code of Practice, statutory clarification of the lawful basis for mandatory biometric collection, a pre-registration privacy-notice requirement, and electoral-specific administrative sanctions, alongside strengthened NDPC oversight of electoral bodies.
- Institutional and operational compliance, including institutionalised privacy governance frameworks, mandatory data protection impact assessments, and standardised privacy notices and consent practices across INEC and the SIECs.
- Enforcement, accountability, and public redress, including more responsive data-subject-rights mechanisms, capacity building and training for electoral officials, and sustained public awareness and voter education on data protection rights.

Conclusion

Nigeria's data protection framework for elections is, on its face, reasonably comprehensive, but institutional practice remains reactive, uneven across tiers of government, and largely unaccompanied by visible enforcement. The study concludes that closing this gap is not a peripheral, technical matter but a constitutive element of electoral integrity itself, and it calls for the recommendations advanced to be implemented as a mutually reinforcing programme so that privacy protection is designed into Nigeria's electoral data ecosystem from the outset of each electoral cycle, rather than extracted from it after the fact.

DEFINITION OF TERMS

For the purposes of this study, the following terms are understood as follows:

Data Protection: The legal, organisational and technical measures adopted to safeguard personal data against unlawful or unauthorised processing, loss, destruction, alteration, access or disclosure, while ensuring that personal data are processed in accordance with applicable legal principles and the rights of data subjects.

Data Transparency: The extent to which an electoral body provides data subjects and other relevant stakeholders with clear, accessible and intelligible information about its collection, use, disclosure, storage, retention and protection of personal data. In this study, data transparency is assessed principally through publicly available institutional documents, privacy notices and policies, websites and other documentary evidence.

Voter Privacy: The protection of the personal information and legitimate privacy interests of persons registered or otherwise participating as voters, including information relating to their identity, contact details, demographic characteristics, biometric information and other personal data processed within the electoral system.

Voter Personal Data: Any information relating to an identified or identifiable voter or prospective voter that is collected, generated, stored, used, transmitted or otherwise processed in connection with electoral activities. This includes identification, demographic and biometric information and other information capable of identifying or being linked to a voter.

Electoral Bodies: Institutions established or authorised by law to administer or conduct elections in Nigeria. In this study, the term principally refers to the Independent National Electoral Commission (INEC) and the State Independent Electoral Commissions (SIECs).

Independent National Electoral Commission (INEC): The constitutionally established federal electoral management body responsible for the organisation and conduct of elections within the scope of its statutory mandate, including the registration of voters and the management of electoral information and technology.

State Independent Electoral Commissions (SIECs): State-level electoral management bodies constitutionally established to organise, undertake and supervise elections to local government councils within their respective states, subject to their constitutional and statutory mandates.

Personal Data: Any information relating to an identified or identifiable individual. For purposes of this study, the term is used consistently with the meaning assigned to it under the Nigeria Data Protection Act 2023 (NDPA).

Sensitive Personal Data: Personal data requiring heightened protection because of its nature and the risks associated with its processing. Within the electoral context, this includes biometric information and other categories of data recognised as sensitive under applicable data-protection law.

Biometric Data: Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual which permit or confirm the unique identification of that individual. In this study, particular attention is given to fingerprints and facial information processed for voter accreditation and identification.

Processing: Any operation or set of operations performed on personal data, whether or not by automated means, including collection, recording, organisation, storage, alteration, retrieval, consultation, use, disclosure, transmission, dissemination, restriction, erasure or destruction.

Data Controller: A person or organisation that, alone or jointly with others, determines the purposes and means of processing personal data.

Data Processor: A person or organisation that processes personal data on behalf of, or under the authority of, a data controller.

Data Subject: An identified or identifiable natural person whose personal data are being processed. In the context of this study, this principally includes registered voters, prospective voters and other individuals whose personal data are processed by electoral bodies.

Data Protection Officer (DPO): A person designated by a data controller or processor to perform data-protection and compliance-related functions, including advising on compliance, monitoring data-protection obligations and serving as a point of contact on relevant data-protection matters.

Data Protection Impact Assessment (DPIA): A systematic assessment undertaken to identify, evaluate and address the potential risks that a proposed or existing processing activity may pose to the rights and freedoms of data subjects, together with measures designed to mitigate those risks.

Personal Data Breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. In this study, the term is preferred to the more general expression "data leak" when referring to a legally relevant breach of personal-data security.

Privacy Notice/Privacy Policy: A publicly accessible statement through which an organisation communicates information concerning its processing of personal data, including the identity of the controller, purposes and lawful basis of processing, categories of data collected, recipients, retention, data-subject rights and available complaint mechanisms.

Lawful Basis: The legally recognised ground upon which personal data may be processed. Under the NDPA, processing may be based on grounds including consent, performance of a contract, compliance with a legal obligation, protection of vital interests, performance of a task carried out in the public interest or in the exercise of official authority, and other applicable lawful grounds.

Consent: A freely given, specific, informed and unambiguous indication of a data subject's wishes by which the data subject signifies agreement to the processing of personal data relating to them, where consent is relied upon as the lawful basis for processing.

Transparency Obligation: The obligation of a data controller or processor to provide data subjects with information concerning the processing of their personal data in a manner that is clear, accessible, intelligible and consistent with applicable data-protection law.

Data Subject Rights: The rights available to individuals in relation to the processing of their personal data, including applicable rights of access, rectification, erasure, restriction, objection, data portability and other rights recognised under the NDPA and applicable regulations.

Bimodal Voter Accreditation System (BVAS): An electronic electoral technology used for voter accreditation and identity verification through biometric modalities, principally fingerprint and facial recognition. In this study, BVAS is examined not only as an electoral technology but also as a system involving the collection, processing, storage and transmission of personal and biometric data.

IReV: The Independent National Electoral Commission's electronic platform for the transmission and public viewing of polling-unit election results. In this study, IReV is examined in the context of the relationship between electoral transparency, public accountability and the protection of personal data.

Electoral Transparency: The availability and accessibility of information concerning the administration, conduct and results of elections in a manner that enables citizens, candidates, political parties, observers and other stakeholders to scrutinise and understand the electoral process.

Electoral Data Lifecycle: The sequence of activities through which personal and other data move within the electoral system, from collection and registration through processing, verification, storage, transmission, disclosure, retention and eventual deletion or disposal.

Compliance: The extent to which an electoral body conforms to applicable legal, regulatory and institutional requirements relating to the collection, processing, protection, disclosure, retention and governance of personal data.

Public-Facing Digital Transparency: The extent to which an electoral body's publicly accessible digital platforms provide clear and readily available information concerning its processing and protection of personal data. In this study, this term specifically relates to information observable through official websites and other publicly accessible digital resources and does not, by itself, establish the existence or absence of internal compliance practices.

Freedom of Information (FOI) Request: A formal request for access to information made pursuant to the Freedom of Information Act 2011. In this study, FOI requests are used as a documentary research tool to obtain information that could not reasonably be established from publicly available sources and to facilitate triangulation of the study's findings.

Compliance Audit Return (CAR): A formal compliance reporting mechanism through which applicable data controllers and processors provide information concerning their data-protection compliance activities to the Nigeria Data Protection Commission in accordance with applicable regulatory requirements.

Nigeria Data Protection Commission (NDPC): The statutory regulatory authority responsible for regulating the processing of personal data and promoting data-protection compliance in Nigeria under the Nigeria Data Protection Act 2023.

General Application and Implementation Directive (GAID) 2025: The regulatory instrument issued by the Nigeria Data Protection Commission to provide detailed requirements and guidance for the implementation and application of the Nigeria Data Protection Act 2023.

Data Controller of Major Importance: A data controller or processor falling within the category recognised under the NDPA and applicable regulatory requirements by reason of the nature, scale or other characteristics of its processing activities, and consequently subject to enhanced registration, compliance and accountability requirements.

VOTER PRIVACY AND UMPIRES' TRANSPARENCY: AN ASSESSMENT OF THE ELECTORAL BODIES' COMPLIANCE WITH THE NIGERIA DATA PROTECTION ACT (NDPA) 2023



CHAPTER 1
INTRODUCTION



1.1 Background to the Study

The right to privacy is a fundamental right recognised and protected under international human rights law and municipal legal systems worldwide.[1] In Nigeria, it is guaranteed under Section 37 of the Nigerian Constitution,[2] which protects the privacy of citizens, their homes, correspondence, telephone conversations, and telegraphic communications.

This constitutional guarantee forms the bedrock upon which data protection norms and principles rest, recognising that in an increasingly digital age, the protection of personal information is not merely a statutory obligation but a constitutional imperative.[3] The intersection of privacy rights and electoral governance presents a unique and complex regulatory challenge. Elections, by their very nature, require the collection, processing, storage, and dissemination of vast quantities of personal data belonging to millions of citizens.[4] Voter registration systems capture sensitive personal information including names, addresses, biometric data (fingerprints and facial images), and other identifiers that, if compromised, could expose citizens to significant harm.[5] The Independent National Electoral Commission (INEC) has been acknowledged to store the largest citizen database in Africa,[6] with over 94 million records from registered voters, including fingerprints and facial biometrics across the executive, legislative, and judicial branches of government.[7] Furthermore, the constitutional protection of privacy under Section 37 has been judicially interpreted to extend beyond physical spaces to encompass personal data and information. The Court of Appeal in Incorporated Trustees of Digital Rights Lawyers Initiative & Ors v. National Identity Management Commission (NIMC)[8] held definitively that the right to privacy under Section 37 extends to the protection of personal data, including communication and personal information. Furthermore, in Nwali v. EBSIEC,[9] the Court of Appeal established the nexus between electoral processes and privacy rights, holding that the privacy of a citizen's choice of candidate and the privacy of voting for that candidate constitute part of the citizen's constitutionally guaranteed privacy. Therefore, the emergence of digital technologies in electoral processes has introduced new dimensions to this constitutional protection. For example, the Bimodal Voter Accreditation System (BVAS), which relies on fingerprint and facial recognition technology to verify voters' identities during elections, processes sensitive biometric data that falls within the category of special personal data under the Nigeria Data Protection Act (NDPA) 2023.[10]

Similarly, the INEC Results Viewing Portal (IReV) and the Continuous Voter Registration (CVR) system process and transmit personal data across digital networks, raising significant questions about transparency, data security, cross-border data transfers, and the rights of data subjects.[11]

The obligation of electoral management bodies to conduct their affairs openly, accountably, and in a manner that engenders public trust in the electoral process is what is conceptualised as "umpire's transparency".[12] Transparency in the context of electoral governance requires that citizens, political parties, civil society organisations, and the media have access to electoral information, including the voters' register, polling unit lists, and other electoral data necessary for monitoring and oversight.[13] However, transparency obligations must be carefully balanced against privacy rights, the right of citizens to have their personal data protected from unauthorised access, disclosure, manipulation and/or misuse. This inherent tension between transparency and privacy lies at the heart of this study.

On one hand, democratic principles demand that electoral processes be transparent to ensure credibility, accountability, and public trust but on the other hand, constitutional and statutory provisions mandate the protection of citizens' personal data from intrusion and misuse.[14] The question that arises is whether Nigeria's electoral bodies have successfully navigated this delicate balance and whether their practices comply with both the letter and spirit of the NDPA 2023.

1.2 Electoral Governance and Personal Data Processing in Nigeria

INEC is the primary electoral management body in Nigeria, established under Section 153 of the 1999 Constitution and empowered by the Electoral Act, 2022 to conduct elections into the offices of the President, Vice-President, Governor, Deputy Governor, the National Assembly, and State Houses of Assembly. INEC is also responsible for the registration of voters, the compilation and maintenance of the National Register of Voters, the conduct of voter education, and the regulation of political parties. In discharging these statutory functions, INEC processes vast quantities of personal data belonging to Nigerian citizens. The voter registration process captures the following categories of personal data:

Footnotes

1 Mubarak Raji, et al, 'An Assessment of the Enforcement Mechanisms in African Data Protection Laws' (2025) 2(1) African Journal on Privacy & Data Protection 1–40.

2 Constitution of the Federal Republic of Nigeria 1999 (as altered), Cap C23, Laws of the Federation of Nigeria 2004.

3 Olumide Babalola, 'Nigeria's Data Protection Legal and Institutional Model: An Overview' (2022) 12(1) International Data Privacy Law 44–52; Festus Okechukwu Ukwueze, 'Strengthening the Legal Framework for Personal Data Protection in Nigeria' (2022) 16(1) The Nigerian Juridical Review 124–142; Emmanuel Tochukwu Okpara and Emmanuella Chidinma Okpara, 'The Nigeria Data Protection Act, 2023 and the Right to Privacy: Constitutional Implications Under the 1999 Nigerian Constitution (As Amended)' (2025) 2 Alex Ekwueme Federal University Law Journal.

4 Colin J Bennett, Personal Data Processing by and for Political Campaigns: The Application of the Council of Europe's Modernised Convention 108 (Council of Europe, T-PD(2020)02, 11 June 2020); Olumide Babalola, 'Data Protection in E-Voting Systems: The 2024 Nigerian Bar Association's Elections in Retrospect' (2025) 13(1) ABUAD Law Journal.

5 Md Jobair Hossain Faruk and others, 'Transforming Online Voting: A Novel System Utilizing Blockchain and Biometric Verification for Enhanced Security, Privacy, and Transparency' (2024) 27 Cluster Computing 4015–4034; Robert Ehimen Okonigene and CE Ojieabu, 'Developed Automated Electoral System Algorithm Using Biometric Data to Eliminate Electoral Irregularities in Nigeria' (2011) 14(6) International Journal of Computer Applications.

6 INEC's publicly available documentation indicates that voter personal and biometric data is stored and processed within Nigeria on its authorised backend infrastructure, while the Commission's 2023 election review confirms that the voters' register is also resident on BVAS devices deployed for election-day accreditation. The INEC data environment therefore appears to involve both central/backend storage and device-level operational storage. See Independent National Electoral Commission, 'Privacy Policy: INEC Personal Biometric Registration Application' (2026) paras 12, 14 https://cvr.inecnigeria.org/privacy; Independent National Electoral Commission, Review of the 2023 General Election (INEC 2024) section 3.8, 'Voting and Result Management'.

7 See Praise Fortune, 'Securing the Ballot: NDPC and INEC Pact to Protect 94 Million Voter Identities' < https://www.techregard.com/securing-the-ballot-ndpc-and-inec-pact-to-protect-94-million-voter-identities/?utm_source> accessed 6 June 2026; Biometricupdate.com, Biometrics used at 98% of Nigerian polls; advocates concerned for safety of voters' data < https://www.biometricupdate.com/202302/biometrics-used-at-98-of-nigerian-polls-advocates-concerned-for-safety-of-voters-data?utm_sourcem> accessed June 6, 2026; deleke S Ogunmokun, Oluwatoyin S Ayanlade and Titilayo O Olaposi, 'An Assessment of the Extent of Adoption of Electoral Technologies in Nigeria's Electoral System' (2024) 11(3) SADI International Journal of Social Science and Humanities; Peter O Eyo, Edem E Edemidiong and Umoh G Tonyudoh, 'Electronic Accreditation and Electoral Administration in Nigeria's 2019 General Elections' (2019) International Journal of Social Sciences; Daramola Joseph Omoyele, 'Election-Day Administrative Barriers and Voter Turnout in Nigeria: Evidence from the 2023 Presidential Election' (2026) SSRN < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=6367178> accessed 6 June 2026.

8 (2021) LPELR-55623(CA); (2022) All FWLR (Pt. 1146), 166.

9 Hon Peter Nwali v. Ebonyi State Independent Electoral Commission (EBSIEC) & Ors. (2014) LPELR-23682(CA)

10 Habiba Musa, 'Data Protection Issues in the Management of the Bimodal Voters Accreditation System (BVAS) in Nigeria' (2023) 10(2) NAU Journal of Commercial and Property Law; Toba Paul Ayeni and Opani Meshark Aweh, 'Examining the Impact of Bimodal Voter Accreditation System (BVAS) as a Game-Changer in Nigeria 2023 Elections' (2023) The Information Technologist: An International Journal of ICT; F S Oladele, 'Technology Security and Electoral Credibility in Nigeria: A National Security Review of BVAS and IReV in the 2023 General Elections' (2025) International Journal of Information and Digital Security; Femi Samuel Oladele, 'Technology Security and Electoral Credibility in Nigeria: A National Security Review of BVAS and IReV in the 2023 General Elections' (2025) 8(3) International Journal of Intellectual Discourse; Adedeji Ogbadebo, 'The Role of BVAS in Safeguarding Electoral Integrity' (2023) Journal of Social Political Sciences.

Data Category	Specific Data Elements	Legal Basis
Identification Data	Full name, date of birth, gender, place of birth	Electoral Act 2022, INEC Regulations and Guidelines
Contact Information	Residential address, occupation (sometimes collected)	Electoral Act 2022
Biometric Data	Fingerprints (all ten digits), facial image	INEC Guidelines, NDPA 2023
Unique Identifiers	Voter Identification Number (VIN), Temporary Voter's Card (TVC), Permanent Voter's Card (PVC)	Electoral Act 2022
Registration History	Previous registration status (new registration, transfer, update)	INEC Regulations

The collection of biometric data, particularly fingerprints and facial images, raises heightened privacy concerns because biometric identifiers are intrinsically sensitive, persistent and closely connected to an individual's identity.[15] Unlike passwords or other conventional identifiers, compromised biometric characteristics cannot readily be replaced, thereby increasing the consequences of unauthorised access, misuse or erroneous identification.[16] The risks are particularly acute where biometric systems are used to determine or verify access to essential legal or social rights. The experience of Kenya illustrates this concern. The litigation and controversy surrounding the Huduma Namba system demonstrate how the centralisation and linking of biometric and identity information can generate significant risks for vulnerable populations where the collection, verification and governance of identity data are inadequate.[17] Similar concerns have arisen in relation to refugees and other vulnerable persons whose biometric information has been captured across different institutional databases, with the potential for erroneous identification, exclusion and difficulties in establishing or maintaining legal identity. Scholarship on biometric registration in Kenya's Kakuma refugee camp similarly demonstrates that biometric infrastructures can extend beyond identification to become mechanisms through which vulnerable populations are rendered more visible, governable and subject to institutional control. These experiences underscore that the data-protection implications of biometric voter registration extend beyond the risk of data breach: they include the risks of misidentification, function creep, excessive data linkage, exclusion and the loss of effective control over information that is intrinsically tied to the individual's identity.

Beyond INEC, State Independent Electoral Commissions (SIECs) conduct local government elections across the 36 states of the federation.[18] These bodies collect and process personal data of citizens within their respective states, though the scale and sophistication of their data processing operations vary considerably. The application of the NDPA 2023 to INEC and SIECs is clear to the extent that they are data controllers within the meaning of the Act, yet research suggests significant gaps in compliance, awareness, and capacity.[19] These gaps are addresses later in this study.

Political parties also play a significant role in electoral data processing. During party primaries, voter registration drives, and campaign activities, political parties collect, store, and process personal data of their members, supporters, and potential voters.[20] Section 31(3) of the NDPA 2023 requires that political parties process personal data of their members in compliance with the Act, including appointing Data Protection Officers (DPOs) and implementing appropriate security measures. However, studies have shown that many political parties remain unaware of or indifferent to their obligations under the NDPA and this is further addressed later here.[21]

1.3 Emergence of Data Protection Regulation in Nigeria

The evolution of data protection regulation in Nigeria reflects a growing recognition of the importance of privacy rights in the digital age. The NDPR[22] was, however, limited in several respects. As a regulation issued by an agency, it lacked the legislative authority of an Act of the National Assembly. Its enforcement mechanisms were limited, and its application to public institutions, including electoral bodies, was not as clearly established as desirable. Recognising these limitations, the National Assembly enacted the Nigeria Data Protection Act (NDPA) 2023, which received presidential assent on 12 June 2023.

The NDPA 2023 represents a comprehensive legislative framework for data protection in Nigeria.[23] The Act establishes the Nigeria Data Protection Commission (NDPC) as the supervisory authority responsible for enforcing the provisions of the Act, investigating complaints, and issuing guidance on data protection practices.
The enactment of the NDPA 2023 was followed by the issuance of the General Application and Implementation Directive (GAID) by the NDPC, which provides detailed guidance on compliance requirements.[24] The GAID, in Article 7, requires data controllers to publish privacy policies on their websites, provide cookie notices that significantly obstruct the homepage, and ensure transparency in data processing activities.

Footnotes

11 Ugo Chuks Okolie, 'BVAS, IReV and Democratic Elections in Nigeria' (2024) Pinisi Journal of Social Science; John Afolabi Ogundengbe and Abdulhafeez Mohammad, 'The Legal Status of the IReV Portal in Nigeria's Electoral Jurisprudence' (2026) University of Ilorin Law Repository; Olasupo O Thompson and others, 'Digital Electoral Reforms and Democratic Consolidation: A Critical Assessment of BVAS and IReV in the 2023 Nigerian General Elections' (2025) Gusau International Journal of Management and Social Sciences;

12 Pippa Norris, 'Transparency in Electoral Governance' in Pippa Norris and Alessandro Nai (eds), Election Watchdogs: Transparency, Accountability and Integrity (Oxford University Press 2017); Toby S James and Holly Ann Garnett, 'Electoral Management and the Organisational Determinants of Electoral Integrity' (2019) 40(3) International Political Science Review 295–312; Holly Ann Garnett, 'Evaluating Electoral Management Body Capacity' (2019) 40(3) International Political Science Review 312–329; Sarah Birch and Carolien van Ham, 'Getting Away with Foul Play? The Importance of Formal and Informal Oversight Institutions for Electoral Integrity' (2017) 56(3) European Journal of Political Research 529–547.

13 Pippa Norris, 'Transparency in Electoral Governance' in Pippa Norris and Alessandro Nai (eds), Election Watchdogs: Transparency, Accountability and Integrity (Oxford University Press 2017); Prashant Agrawal and others, 'Publicly Auditable Privacy-Preserving Electoral Rolls' (2024) arXiv:2402.11582 https://arxiv.org/abs/2402.11582 accessed 6 June 2026;

14 Ziaul Haque and David P Carroll, 'Assessing the Impact of Information and Communication Technologies on Electoral Integrity' (2020) 19(2) Election Law Journal 111–126; E Scott Adler and Thad E Hall, 'Ballots, Transparency, and Democracy' (2013) 12(2) Election Law Journal 123–140; Toby S James and Holly Ann Garnett, 'The Determinants of Electoral Registration Quality: A Cross-National Analysis' (2023) 43 Representation 279–302; Prashant Agrawal and others, 'Publicly Auditable Privacy-Preserving Electoral Rolls' (2024) arXiv:2402.11582 https://arxiv.org/abs/2402.11582 accessed 6 June 2026.

15 The collection of biometric data, particularly fingerprints and facial images, raises heightened privacy concerns because biometric identifiers are intrinsically sensitive, persistent and closely connected to an individual's identity. Unlike passwords or other conventional identifiers, compromised biometric characteristics cannot readily be replaced, thereby increasing the consequences of unauthorised access, misuse or erroneous identification. The risks are particularly acute where biometric systems are used to determine or verify access to essential legal or social rights. The experience of Kenya illustrates this concern. The litigation and controversy surrounding the Huduma Namba system demonstrate how the centralisation and linking of biometric and identity information can generate significant risks for vulnerable populations where the collection, verification and governance of identity data are inadequate. Similar concerns have arisen in relation to refugees and other vulnerable persons whose biometric information has been captured across different institutional databases, with the potential for erroneous identification, exclusion and difficulties in establishing or maintaining legal identity. Scholarship on biometric registration in Kenya's Kakuma refugee camp similarly demonstrates that biometric infrastructures can extend beyond identification to become mechanisms through which vulnerable populations are rendered more visible, governable and subject to institutional control.[1] These experiences underscore that the data-protection implications of biometric voter registration extend beyond the risk of data breach: they include the risks of misidentification, function creep, excessive data linkage, exclusion and the loss of effective control over information that is intrinsically tied to the individual's identity.

16 Simon Hanisch, Julian Todt, José Patino, Nicholas Evans and Thorsten Strufe, 'A False Sense of Privacy: Towards a Reliable Evaluation Methodology for the Anonymization of Biometric Data' (2023) arXiv:2304.01635; Marcus Smith and Seumas Miller, 'The Ethical Application of Biometric Facial Recognition Technology' (2021) AI & Society 37(1) 167–175; Meng Wang and others, 'Identifying Personal Physiological Data Risks to the Internet of Everything: The Case of Facial Data Breach Risks' (2023) Humanities and Social Sciences Communications 10:216; Marta Gómez-Barrero and Javier Galbally, 'Reversing the Irreversible: A Survey on Inverse Biometrics' (2024) arXiv:2401.02861.

In July 2025, President Bola Ahmed Tinubu directed all Ministries, Extra-Ministerial Departments, and Agencies to comply with the provisions of the NDPA 2023, describing data as the "new oil" whose value increases and needs to be refined and responsibly shared.[25] This directive underscored the executive commitment to data protection compliance across the public sector, including electoral bodies.

In April 2026, the NDPC inaugurated a joint NDPC–INEC working group aimed at embedding robust data protection and privacy practices across Nigeria's electoral ecosystem.[26] The partnership focuses on several core areas, including the establishment of a joint working group to oversee data protection compliance, enhanced voter data security safeguards, mandatory appointment of Data Protection Officers (DPOs) by political parties, training and certification of INEC staff on ISO 27701 Privacy Information Management System (PIMS), and enforcement measures with penalties ranging from N10 million to up to 2% of gross annual earnings.[27] Despite these positive developments, significant compliance gaps remain. A 2025 investigation revealed that several government agencies, including INEC, lacked privacy policies and cookie notices on their websites, months after the President's compliance directive. This clearly constitutes a contravention of the NDPA and the GAID, which require transparent information about data processing activities at the point of collection.[28]

1.4 Statement of the Problem

Notwithstanding the comprehensive legal framework established by the NDPA 2023 and the collaborative efforts between the NDPC and INEC, evidence suggests significant gaps in electoral bodies' compliance with data protection obligations.[29] These gaps manifest in several troubling dimensions:

First, data breaches involving voter information have occurred and continue to pose risks to citizens' privacy. In June 2026, the Centre for Justice and Development (CJID) condemned a data breach at INEC involving the alleged disclosure of personal voter data obtained from the Commission's database.[30] Second, there have been allegations of unauthorised use of voter data for political purposes. In April 2025, the Transition Monitoring Group (TMG) called on the NDPC to investigate the alleged unauthorised and fraudulent use of personal data of constituents in the failed recall attempt of Senator Natasha Akpoti-Uduaghan representing Kogi Central Senatorial District.[31] Flowing from this, there were concerns that the personal information of voters may have been illegally harvested and deployed without their consent in a bid to generate signatures for the recall petition.

Third, INEC's compliance with transparency obligations under the NDPA remains questionable. The absence of privacy policies and cookie notices on INEC's website, as documented in 2025, suggests a lack of basic transparency in data processing activities. Commentators have noted that this absence is not a mere irregularity but a clear contravention of extant legislation and regulation.[32] If a data controller of major importance such as INEC cannot meet the foundational transparency requirements of the NDPA, what confidence can citizens have in the protection of their sensitive biometric data?

Fourth, the tension between transparency and privacy has not been adequately resolved. In October 2025, the Media Rights Agenda (MRA) criticised INEC for demanding a fee of over N1.5 billion for a copy of the National Register of Voters and the list of polling units, describing the demand as an attempt to "weaponise cost" and deny public access to vital electoral information.[33] While INEC may justify such fees as necessary to prevent misuse of voter data or to recoup administrative costs, the Freedom of Information Act, 2011 mandates that fees for access to public records be limited to the standard cost of duplication. This incident highlights the unresolved tension between electoral transparency (which requires public access to voter data for monitoring and oversight) and data protection (which requires restrictions on access to prevent misuse).

Fifth, the compliance of State Independent Electoral Commissions (SIECs) with the NDPA has not been systematically assessed. While INEC has been the primary focus of policy attention, SIECs across the 36 states process voter data for local government elections. The extent of their compliance with the NDPA, including the appointment of DPOs, implementation of security measures, and respect for data subject rights, remains largely unknown.[34] Sixth, there is a significant gap between the law and the reality of data protection for voters. The NDPA confers extensive rights on data subjects, including the right to access personal data, the right to rectification, and the right to lodge complaints with the NDPC. However, the extent to which Nigerian voters are aware of these rights and the extent to which they can practically exercise them remains unexamined.

This study is therefore motivated by the need to assess the compliance of electoral bodies with the NDPA. By examining the practices of INEC and SIECs in relation to voter data collection, processing, storage, sharing, and transparency, this study seeks to identify compliance gaps, assess the effectiveness of existing regulatory mechanisms, and propose evidence-based recommendations for reform.

Footnotes

17 For the Kenyan Huduma Namba litigation specifically, see Nubian Rights Forum v Attorney General [2020] eKLR, where the High Court considered the legality and constitutional implications of the Huduma Namba system, including the collection and processing of biometric and other identity information. Haki na Sheria Initiative, 'Biometric Purgatory: How the Double Registration of Vulnerable Kenyan Citizens in the UNHCR Database Left Them at Risk of Statelessness' (Citizenship Rights in Africa, 2026) https://citizenshiprightsafrica.org/en/biometric-purgatory-how-the-double-registration-of-vulnerable-kenyan-citizens-in-the-unhcr-database-left-them-at-risk-of-statelessness accessed 11 August 2026; Giuseppe Iazzolino, 'Infrastructure of Compassionate Repression: Making Sense of Biometrics in Kakuma Refugee Camp' (2021) 27(1) Information Technology for Development 111; Katri Weitzberg, 'Keeping People Out of Camps: Biometric Technologies, Contested Sovereignty, and Border Practices within Humanitarian Spaces' (2025) 51(14) Journal of Ethnic and Migration Studies 3590.

18 Johnson O Olaniyi, 'State Independent Electoral Commissions and Local Government Elections in Nigeria' (2017) 5(1) Africa's Public Service Delivery and Performance Review e133; Severus I Odoziobodo and Hyginus B Okibe, 'Between Illusion and Reality: Interrogating the Independence of State Independent Electoral Commissions in Nigeria' (2018) International Journal of Advanced Research in Public Policy, Administration and Development Strategies; Abacha Umar Deribe, Usman Sambo, Babayo Sule and Ibrahim Salihu, 'Unmasking the Tape of Electoral Fraud in Grassroots Nigeria: Evidence from the Management of Local Council Elections by State Independent Electoral Commissions' (2022) 1(1) Middle East Research Journal of Humanities and Social Sciences 25–37.

19 Ugo Chuks Okolie, 'Data Protection Governance in Nigeria: Challenges of Implementation under the Nigeria Data Protection Act 2023' (2024) Journal of African Law and Digital Policy; Toby S James and Holly Ann Garnett, 'The Determinants of Electoral Registration Quality: A Cross-National Analysis' (2023) 43 Representation 279–302; Chinedu Ndubuisi, 'Data Protection Enforcement in Emerging Economies: Institutional Challenges in Africa' (2023) African Journal of Information Systems; Sarah Birch and Carolien van Ham, 'Getting Away with Foul Play? The Importance of Formal and Informal Oversight Institutions for Electoral Integrity' (2017) 56(3) European Journal of Political Research 529–547; Tunji Akomolede, 'Implementing the Nigeria Data Protection Act 2023: Challenges and Prospects' (2024) Nigerian Journal of Technology and Law.

20 Colin J Bennett, 'Personal Data Processing by and for Political Campaigns: The Application of the Council of Europe's Modernised Convention 108' (2020) SSRN Working Paper; Hashim Mude, 'Political Micro-Targeting in Kenya: An Analysis of the Legality of Data-Driven Campaign Strategies under the Data Protection Act' (2021) 1(1) Journal of Intellectual Property and Information Technology Law 7–36; Maja Brkan, 'EU Fundamental Rights and Democracy Implications of Data-Driven Political Campaigns' (2020) 27(6) Maastricht Journal of European and Comparative Law;.

21 See Timi Olagunju, 'How INEC and Nigeria's Major Parties Are Failing the First Test of Digital Democracy'

<https://www.techpolicy.press/how-inec-and-nigerias-major-parties-are-failing-the-first-test-of-digital-democracy/> Access June 6, 2026; Epiphanus Obia, 'Ahead of 2027, Nigerian political parties are harvesting sensitive citizen data without transparency' < https://itpulse.com.ng/ahead-of-2027-nigerian-political-parties-are-harvesting-sensitive-citizen-data-without-transparency/> Accessed 6 June 2026.

22 The Nigeria Data Protection Regulation 2019 was sidestepped by the NDPA General Application Implementation Directive 2025. See Stephanie Modilim, Iyanuoluwa Bolarinwa, Motunrayo Tolani Omidiora and Obah Tawo, "Reforming Data Governance in Nigeria: A Critical Analysis of the Nigeria Data Protection Act, Regulatory Enforcement, and Global Alignment" (2024) 7 International Journal of Law Management & Humanities 2481–2495; Patrick Chukwunonso Aloamaka, "A Critical Analysis of the Nigeria Data Protection Act 2023: Elevating Standards to Global Norms" (2025) 4(2) UCC Law Journal 242–263; Opeyemi Shokunbi, Michael Agbaje and Emmanuel C. Ogu, "Measuring Nigeria Data Protection Act (NDPA) 2023 Compliance in Nigerian Universities: A General Compliance Index and Evidence of Institutional Decoupling" (2026) FUDMA Journal of Sciences.

1.5 Objectives of the study

This study is designed to achieve the following objectives:

To assess the compliance of Nigeria's electoral bodies, specifically the INEC and SIEC, with the provisions of the Nigeria Data Protection Act (NDPA) 2023 regarding the collection, processing, storage, protection, and transparency of voter personal data.

To examine how electoral bodies can improve compliance with the NDPA by strengthening transparency requirements on their digital platforms, including the publication of privacy policies, cookie notices, and clear information on data processing activities. It also seeks to identify the key compliance gaps, operational challenges, and institutional barriers that hinder effective implementation of the NDPA within electoral administration.

In addition, the research analyses the inherent tension between electoral transparency, particularly public access to voter data and the imperative of protecting voter privacy, with the aim of proposing a balanced framework that reconciles these competing values. Building on this analysis, it offers evidence-based recommendations to enhance regulatory compliance by electoral bodies, improve voter awareness of data protection rights, and strengthen enforcement mechanisms within Nigeria's electoral and data governance systems.

1.6 Scope and Limitations

This study is delimited to the assessment of electoral bodies' compliance with the NDPA. The geographical scope covers Nigeria, with a specific focus on INEC at the federal level and selected State Independent Electoral Commissions (SIECs) across the six geopolitical zones of the federation: North-West, North-East, North-Central, South-West, South-East, and South-South.

The substantive scope of the study covers:

Dimension	Specific Focus
Legal Framework	NDPA 2023, GAID, and relevant constitutional provisions
Data Protection Principles	Lawfulness, transparency, integrity and confidentiality
Data Subject Rights	Right to be informed, right of access
Transparency Obligations	Privacy policies, cookie notices, data processing information, FOI compliance
Security Measures	Technical and organisational measures to protect voter data from unauthorised access, disclosure, alteration, or destruction
Breach Management	Detection, investigation, notification to NDPC, communication to affected data subjects

The temporal scope covers the period from the enactment of the NDPA in June 2023 to the present (June 2026), with particular attention to developments post-2025 when the Presidential directive on compliance was issued.

Limitations:

This study acknowledges several inherent limitations that affect the scope, depth, and generalizability of its findings. These limitations relate to data access, geographical coverage, methodological challenges, and the novelty of the legal framework under investigation.

First, access to internal records of electoral bodies presents a significant challenge. SIECs and INEC may be reluctant to disclose internal data protection policies, breach reports, or compliance audits due to institutional confidentiality protocols or concerns about public accountability. To mitigate this limitation, the study relies on publicly available documents, Freedom of Information (FOI) requests, and any information voluntarily disclosed by the commissions (if any). Where FOI requests are unsuccessful or only partially honoured, the study will triangulate available data from alternative credible sources.

Second, the reluctance of key informants may constrain the depth of qualitative insights. Officials of electoral bodies and the NDPC may hesitate to speak candidly about compliance failures, institutional gaps, or data breaches due to institutional, political, or legal sensitivities. Fear of professional repercussions or reputational damage could lead to guarded responses or outright refusal to participate. To address this, the study will guarantee anonymity for all informants who request it, ensuring that no identifying information is disclosed in the final report. Additionally, the study will employ data triangulation by cross-referencing interview responses with documentary evidence, media reports, and civil society investigations, such as those conducted by SERAP, to validate findings and reduce reliance on any single source.

Finally, the absence of judicial precedents interpreting the NDPA in the context of electoral bodies constitutes a legal limitation. As the NDPA was enacted only in June 2023, it remains a relatively recent piece of legislation. Consequently, there are no readily available specific Nigerian judicial decisions that interpret its provisions, establish binding precedents, or clarify ambiguities specifically as they apply to SIECs or electoral data processing. This lack of case law limits the study's ability to assess how courts might resolve disputes concerning SIEC compliance, data breaches, or enforcement actions. Despite these limitations, the study is designed to produce robust, credible, and actionable findings.

Footnotes

23 A.I. Uwadinma, "The Digital Economy and Consumer Protection in Nigeria: A Legal Analysis of Data Privacy Laws under the Nigeria Data Protection Act 2023" (2025) AUN Journal of Law; Rilwan F. Mahmoud, Eeman Yusuf and Mamudat Olohungbebe, "Blockchain and Data Privacy in Nigeria: Reconciling Innovation with the Nigeria Data Protection Act 2023" (2025) 19(2) Agora International Journal of Juridical Sciences; Safiyyah Ummu Mohammed, "Human Rights and Algorithmic Accountability under the Nigeria Data Protection Act 2023" (2026) 6(1) Scholarly Journal of Advanced Legal Research; Emmanuel Tochukwu Okpara and Emmanuella Chidinma Okpara, "The Nigeria Data Protection Act, 2023 and the Right to Privacy: Constitutional Implications under the 1999 Nigerian Constitution (as Amended)" (2025) 2 Alex Ekwueme Federal University Law Journal.

24 Nabil Ogirima Abubakar, "The Data Protection Impact Assessments (DPIAs) under GAID 2025: When are they Mandatory?" (2026) SSRN Working Paper; Simon Victor Ugbedeojo, "Digital Footprints and Data Ownership in Nigeria: Reconciling Control under the NDPA and GAID" (2025) SSRN Working Paper; Honour Dahunsi, "Examining Nigeria's Data Protection and Processing Frameworks: Obligations, Breaches and Cross Border Data Transfers" (2025) SSRN Working Paper. https://ssrn.com/abstract=5368622 ; Muiz Adeleke, "NDP Act GAID Simplified: From Confusion to Compliance" (2025) ResearchGate Working Paper (Deloitte & Touche). https://www.researchgate.net/publication/396657319; Dr Vincent Olatunji, "The General Application and Implementation Directive (GAID): Operationalising the Nigeria Data Protection Act, 2023" (2026) NDPC Journal Publication.

25 The Punch, Tinubu declares data Nigeria's new oil, says it's key to progress < https://punchng.com/tinubu-declares-data-nigerias-new-oil-says-its-key-to-progress/> Accessed on 10 June 2026.

26 NDPC, INEC partner to protect voter data ahead of Nigeria's 2027 elections < https://www.itedgenews.africa/ndpc-inec-partner-to-protect-voter-data-ahead-of-nigerias-2027-elections/#mnmd-offcanvas-mobile> Accessed June 10, 2026; Technology Times, 'NDPC, INEC target data protection for 94m voters before 2027 elections' < https://technologytimes.ng/ndpc-inec-target-data-protection-for-94m-voters/?utm_source> Accessed June 10, 2026.

27 Leadership News, NDPC, INEC, Move to Strengthen Election Data Protection Measures

28 Nnaemeka Onyekachi, 'Nigerian agencies breach data law despite Tinubu's directives on Privacy' < https://nairametrics.com/2025/09/17/nigerian-agencies-breach-data-law-despite-tinubus-directives-on-privacy/?> Accessed 9 June 2026.

29 INEC Admits Wike's Aide Had Access to Voter Data, Commences Probe < https://www.newswatch.com.ng/inec-admits-wikes-aide-had-access-to-voter-data-commences-probe/> Accessed 9 June 2026; Priscilla Iwedike, 'DSS joins investigation as INEC traces voter data leak to insider access' < http://guardian.ng/news/dss-joins-investigation-as-inec-traces-voter-data-leak-to-insider-access/> Accessed 9 June 2026.

30 CJID Condemns Data Breach At INEC Raises Serious Privacy and Data Protection Concerns' <https://thecjid.org/cjid-condemns-data-breach-at-inec-raises-serious-privacy-and-data-protection-concerns/?> Accessed 10 June 2026.

31 Sodiq Omolaoye, Group demands probe of alleged data breach in Natasha's failed recall < https://guardian.ng/news/group-demands-probe-of-alleged-data-breach-in-natashas-failed-recall/?> Accessed 9 June 2026.

32 Nnaemeka Onyekachi, 'Nigerian agencies breach data law despite Tinubu's directives on Privacy' < https://nairametrics.com/2025/09/17/nigerian-agencies-breach-data-law-despite-tinubus-directives-on-privacy/?> Accessed 9 June 2026.

33 Silver Nwokoro, MRA, INEC differ on N1.5 billion fee for FOI request < https://guardian.ng/news/mra-inec-differ-on-n1-5-billion-fee-for-foi-request/> Accessed 9 June 2026; Ruth Natsa, MRA faults INEC's 1.5bn voters register fee says it undermines transparency' < https://businessday.ng/news/article/mra-faults-inecs-%E2%82%A61-5bn-voters-register-fee-says-it-undermines-transparency/?> Accessed 9 June 2026.

34 Titilope Joseph, 'SERAP Gives Govs Seven Days To Disclose Details Of SIEC Members, Others' < https://independent.ng/serap-gives-govs-seven-days-to-disclose-details-of-siec-members-others/> Accessed 9 June 2026; Human and Environmental Development Agenda (HEDA Resource Centre), 'From Apathy To Action A Reform Blueprint For SIECs & Community-Level Democracy Lar, Volume (5), Issue (2), June 2025 < https://hedang.org/wp-content/uploads/2025/07/LAR-2ND-EDITION-new-version.pdf> Accessed 9 June 2026.

The study will manage these limitations through a combination of data triangulation, alternative sources of evidence, ethical safeguards and comparative legal analysis.

First, where access to internal records of INEC and SIECs is restricted or not granted, the study will rely on publicly available documents, Freedom of Information (FOI) requests, official publications, privacy policies, regulatory materials and other credible secondary sources. Where FOI requests are unsuccessful or responses are incomplete, information from multiple independent sources will be triangulated to strengthen the reliability of the findings.

Second, to address potential reluctance among key informants, the study will ensure confidentiality and, where requested, anonymity. Interviews will be supplemented by documentary evidence, regulatory publications, media reports and credible civil-society investigations. This triangulation will reduce reliance on individual accounts and help identify inconsistencies or gaps in responses.

Third, the limited body of Nigerian judicial decisions interpreting the NDPA in the electoral context will be addressed through doctrinal and comparative analysis. The study will examine the text of the NDPA, applicable regulations and guidance issued by the NDPC, relevant Nigerian privacy and electoral jurisprudence, and persuasive decisions and regulatory approaches from other jurisdictions. This will provide a broader legal basis for analysing unresolved questions while clearly distinguishing binding Nigerian authority from comparative and persuasive materials.

Finally, the study will acknowledge evidential and methodological gaps rather than infer conclusions where reliable evidence is unavailable. By combining evidence with doctrinal and comparative analysis, the study seeks to produce findings that are credible, transparent and sufficiently robust despite the identified limitations.

1.7 Methodology and Sources of Data

The study adopts a documentary research methodology combining the systematic analysis of publicly available documents with targeted requests for information made under the Freedom of Information Act 2011. The documentary component covers publicly accessible primary and secondary materials relevant to the processing and protection of voter personal data by electoral management bodies. These materials include legislation and subsidiary regulations, regulatory guidance and publications, official reports, policy documents, privacy notices, compliance and audit materials where publicly available, institutional websites and publications, electoral technology documentation, court decisions, academic literature, and other authoritative documents published by INEC, SIECs, the Nigeria Data Protection Commission (NDPC) and other relevant institutions.

The study also undertook a structured investigation of the official websites of INEC and the 36 SIECS for availability. The website review was conducted using a common audit protocol applied consistently across all 36 SIECs. The assessment focused on publicly observable indicators of data-protection transparency, including the availability and accessibility of privacy policies or notices and the prescribed contents.

To supplement the publicly available documentary evidence, the study submitted targeted Freedom of Information requests to selected regulatory and public institutions. The requests sought information that could not reasonably be established from publicly available sources, particularly concerning institutional compliance, regulatory oversight, audits, complaints, enforcement activity, data-protection governance and related accountability mechanisms. The FOI component was therefore used as a means of triangulating publicly available evidence and identifying information gaps, rather than as a substitute for documentary analysis.

Each FOI request was framed around specific information relevant to the research questions and, where appropriate, requested documentary evidence supporting the information provided. Responses received were reviewed alongside the relevant legislation, regulatory materials, institutional publications and other documentary sources. Where a request was unanswered, partially answered, declined or otherwise unsuccessful, this was recorded as part of the research process and was not treated automatically as evidence that the underlying activity or practice did not exist. An absence of information was distinguished from evidence of non-compliance.

The study employs a source-verification and triangulation approach. Claims concerning legal obligations were assessed primarily against applicable legislation and regulations; claims concerning institutional practice were assessed against official institutional documents and, where available, responses to FOI requests; while academic literature was used to contextualise and critically evaluate the legal and institutional findings. Where information obtained from different sources conflicted, the study considered the authority, date, provenance and specificity of each source before reaching a conclusion. The methodology is consequently directed principally at assessing publicly observable compliance, transparency and institutional accountability, rather than making unsupported assertions about internal processing practices that cannot be verified from available evidence.

In particular, the absence of a publicly available privacy policy, audit report, DPIA, compliance document or other record is treated as evidence of an information or transparency gap, rather than conclusive proof that the relevant document or compliance activity does not exist. Where the study concludes that an electoral body appears not to have complied with a particular statutory obligation, that conclusion is based on the available documentary evidence and is expressed subject to the limitations inherent in documentary and FOI-based research.

Generative Artificial Intelligence (GenAI) tools[35] were used in the preparation of this study for limited editorial and conceptual-support purposes. Specifically, the researchers used GenAI to assist in framing, organising and refining preliminary thoughts, questions and possible lines of inquiry during the development of the study.

GenAI was not used to generate the substantive content of the study, including its research findings, analysis, arguments, interpretations, conclusions or recommendations. The researchers independently conducted the research, reviewed and evaluated the relevant sources, determined the methodology, analysed the evidence and developed the arguments and conclusions presented in this study. All substantive content was therefore subject to the researchers' independent judgment and verification. The use of GenAI was limited to an editorial aid and did not replace the researchers' intellectual contribution, scholarly judgment or responsibility for the accuracy and integrity of the work.

Footnotes

35 ChatGPT-4.0 and Claude AI were used during the preparation of this study solely as editorial and ideational aids. They were used to assist the researchers in framing, organising and refining preliminary thoughts, questions and lines of inquiry. Neither tool was used to generate the substantive content of the study, including its research findings, analysis, assessments, legal arguments, conclusions or recommendations.

CHAPTER 2
ELECTORAL BODIES AND DATA PROCESSING OPERATIONS IN NIGERIA

VOTER PRIVACY AND UMPIRES' TRANSPARENCY: AN ASSESSMENT OF THE ELECTORAL BODIES' COMPLIANCE WITH THE NIGERIA DATA PROTECTION ACT (NDPA) 2023



Electoral administration in Nigeria increasingly depends on the collection, processing, storage and transfer of personal data. The conduct of elections requires electoral bodies to obtain and manage substantial volumes of information relating to voters, candidates, electoral officials and other participants in the electoral process. The increasing deployment of biometric registration systems, electronic accreditation and result-management platforms has further expanded the scale and complexity of electoral data processing.

This chapter examines the institutional structure and statutory mandates of the INEC and SIECs, with particular attention to their functions as data controllers under Nigeria's data protection framework. It considers the constitutional and statutory foundations of these bodies, their operational capacities, and the nature and categories of personal data processed in the discharge of their electoral functions.

The chapter further examines the principal stages and systems through which voter data is processed, including voter registration, biometric data collection, the Bimodal Voter Accreditation System (BVAS), the INEC Result Viewing Portal (IReV) and the National Voter Register. It considers the data flows associated with these systems and the resulting implications for privacy, security, transparency and accountability. Particular attention is given to the processing of biometric and other sensitive personal data and the circumstances in which such processing may require enhanced safeguards, including a Data Protection Impact Assessment.

Finally, the chapter considers the broader electoral data-processing ecosystem, including the involvement of technology vendors and other third-party processors. It examines the legal and practical implications of sharing voter data with such entities and the obligations imposed on processors under the NDPA. By mapping the institutions, data categories, processing activities, technological infrastructure and third-party relationships involved in electoral administration, the chapter provides the factual and institutional foundation for evaluating the compliance of Nigerian electoral bodies with data-protection requirements.

2.1 Structure and Mandate of the Independent National Electoral Commission (INEC)

INEC is the primary electoral management body in Nigeria, established under Section 153 of the Constitution of the Federal Republic of Nigeria, 1999. Its powers and functions are further elaborated in Part I of the Third Schedule to the Constitution and the Electoral Act, 2022 (as amended).

2.1.1 Constitutional and Statutory Mandate

INEC's core mandate is derived from both the Constitution of the Federal Republic of Nigeria and the Electoral Act 2022, and spans six principal functions[36] First, under section 9 of the Electoral Act 2022, the Commission is charged with conducting continuous voter registration and maintaining the National Register of Voters. Second, by virtue of the Third Schedule to the Constitution, INEC organises and supervises elections for the President and Vice-President, State Governors, members of the National Assembly, and members of State Houses of Assembly. Third, Part III of the Electoral Act 2022 empowers the Commission to register and regulate political parties, including monitoring their finances and conventions. Fourth, the Commission is mandated under the Electoral Act 2022 to conduct voter education programmes and disseminate electoral information to the public. Fifth, section 74 of the Constitution assigns to INEC the responsibility of reviewing and delineating constituency boundaries.[37] Finally, the Commission is responsible for the collation of election results and the declaration of winners, a function equally grounded in the Electoral Act 2022. Together, these functions position INEC as the central institution for the administration and integrity of Nigeria's electoral process.[38]

2.1.2 INEC as a Data Controller of Major Importance

Under the NDPA, INEC qualifies as a data controller of major importance due to the scale, sensitivity, and public interest nature of its data processing activities.[39] The NDPC has recognised that INEC holds one of the largest repositories of personal data in the country with over 94 million registered voter records, including biometric data.[40] This designation carries enhanced obligations under the NDPA, including mandatory registration with NDPC, appointment of a Data Protection Officer (DPO), conduct of Data Protection Impact Assessments (DPIAs) for high-risk processing, enhanced breach notification obligations, potential liability for fines up to N10 million or 2% of annual gross revenue.[41]

2.1.3 Financial and Operational Autonomy under the Electoral Act 2026

The Electoral Act 2026 introduced significant reforms aimed at strengthening INEC's operational independence. A key provision is the establishment of a dedicated INEC Fund, which mandates the release of election funds at least six months before polls. This financial autonomy is critical for data protection compliance, as it should enable INEC to invest in secure data storage and encryption infrastructure, regular security audits and penetration testing, staff training on data protection (including ISO 27701 Privacy Information Management System certification, as established under the NDPC–INEC partnership), Data Protection Officer (DPO) office and resources

Footnotes

36 Nwamaka Adaora Iguh, 'The Legal Burden on the Independent National Electoral Commission (INEC) by the Electoral Act 2022' (2023) 5(2) International Review of Law and Jurisprudence 1.

37 Yahaya Alhaji Dunoma and Baba Isa Sanda Benisheikh, 'An Overview of the Electoral Act, 2022' (2023) 7(6) International Journal of Research and Innovation in Social Science 1505–1522

38 Abdulrahman Abubakar, Electoral Administration and the Role of the Independent National Electoral Commission (INEC) in Nigeria's 2023 General Elections (Covenant University Journal of Politics and International Affairs, 2025).

39 Section 65 of the NDPA defines data controller of major importance as: "a data controller that is domiciled, resident in, or operating in Nigeria and processes or intends to process personal data of more than such number of data subjects who are within Nigeria, as the Commission may prescribe, or such other class of data controller or data processor that is processing personal data of particular value or significance to the economy, society or security of Nigeria as the Commission may designate.

40 NDPC, INEC partner to protect voter data ahead of Nigeria's 2027 elections < https://www.itedgenews.africa/ndpc-inec-partner-to-protect-voter-data-ahead-of-nigerias-2027-elections/#mnmd-offcanvas-mobile> Accessed June 10, 2026; Technology Times, 'NDPC, INEC target data protection for 94m voters before 2027 elections' < https://technologytimes.ng/ndpc-inec-target-data-protection-for-94m-voters/?utm_source> Accessed June 10, 2026.

41 See sections 28, 32(1), 44(1) and 48 NDPA.

2.2 Structure and Mandate of SIECs

2.2.1 Constitutional Foundation

The SIECs are established under Section 197(1)(b) of the 1999 Constitution, with their composition and powers set out in Part II of the Third Schedule. Each of Nigeria's 36 states has an SIEC responsible for conducting local government elections, which produce 768 local government chairmen and 8,747 councillors, totalling 9,515 constituency positions across the federation.[42]

2.2.2 SIECs as Data Controllers under the NDPA

The NDPA applies equally to SIECs as data controllers. However, the Act's tiered compliance framework recognises that not all data controllers have the same capacity. Since SIECs also handle political data, then they are classified data controllers of major importance, and the levels will depend on the volume and sensitivity of data they process. Notwithstanding these distinctions, SIECs remain fully subject to the core data protection principles in Section 24 of the NDPA, including lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, security, and accountability.

2.2.3 Operational Challenges and Capacity Constraints

Despite their constitutional mandate, SIECs face significant operational challenges that directly impact their ability to comply with data protection obligations under the NDPA 202. Some available reports[43] revealed several systemic deficiencies:

Challenge	Implication for Data Protection
Lack of functional offices in local government areas	Decentralised voter data may be vulnerable to unauthorised access or loss
Inability to recruit permanent staff	Data protection responsibilities may be handled by temporary or untrained personnel
Commissions not properly constituted or lacking security of tenure	Absence of institutional continuity for data protection governance
SIECs constituted only on the eve of elections and dissolved thereafter	No sustained data protection framework; processing occurs in rushed, insecure environments
Severe under-resourcing	Inadequate funding for secure data storage, encryption, staff training, or DPO appointment

The Forum of State Independent Electoral Commissions of Nigeria (FOSIECON) has acknowledged these challenges and advocated for strengthening rather than abolishing SIECs.[44]

Facing these realities, many SIECs may be unable to meet even the baseline requirements of the NDPA 2023, particularly regarding lawful basis documentation for voter data processing, security measures to protect sensitive personal data, data subject rights implementation (access, rectification, complaints), and data breach notification procedures.

2.3 Categories of Personal Data Processed by Electoral Bodies

Electoral bodies in Nigeria process extensive categories of personal data. Understanding these categories is essential for assessing NDPA compliance, as different data types carry different risk profiles and legal requirements.

2.3.1 General Personal Data

Data Category	Specific Elements	Processed By	Legal Basis
Identification Data	Full name, date of birth, gender, place of birth	INEC, SIECs	Electoral Act 2022
Contact Information	Residential address, phone number, email address	INEC (primarily)	Electoral Act 2022
Unique Identifiers	Voter Identification Number (VIN), Temporary Voter's Card (TVC), Permanent Voter's Card (PVC), National Identification Number (NIN)	INEC	Electoral Act 2022
Registration History	New registration, transfer, update, previous voting status	INEC	INEC Regulations

2.3.2 Sensitive Personal Data (Biometric Data)

Under the NDPA, biometric data is classified as sensitive personal data requiring enhanced protection.[45] The Act defines sensitive personal data as including "personal data relating to an individual's genetic and biometric data, for the purpose of uniquely identifying a natural person, race or ethnic origin, religious or similar beliefs, such as those reflecting conscience or philosophy, health status, sex life, political opinions or affiliations, trade union memberships etc."[46]

Footnotes

42 Johnson O Olaniyi, 'State Independent Electoral Commissions and Local Government Elections in Nigeria' (2017) 5(1) Africa's Public Service Delivery and Performance Review 1; Severus I Odoziobodo and Hyginus B Okibe, 'Between Illusion and Reality: Interrogating the Independence of State Independent Electoral Commissions in Nigeria' (2018) 6(1) International Journal of Advanced Research in Public Policy, Administration and Development Strategies; Abacha Umar Deribe, Usman Sambo, Babayo Sule and Ibrahim Salihu, 'Unmasking the Tape of Electoral Fraud in Grassroots Nigeria: Evidence from the Management of Local Council Elections by the State Independent Electoral Commissions (SIECs)' (2022) 4(1) Kashere Journal of Humanities, Management and Social Sciences.

43 See Gift Habib, 'Governors have turned LG elections to 'mere coronation' – INEC chair' <https://punchng.com/governors-have-turned-lg-elections-to-mere-coronation-inec-chair/?utm_source=auto-read-also&utm_medium=web> Accessed 10 June 2026; Yakubu, M. (2024) 'Let SIECs Be', Vanguard, 5 June. Available at: https://www.vanguardngr.com/2024/06/let-siecs-be/ (Accessed: 13 June 2026); Sodiq Omolaoye, 'INEC Knocks SIECs, Likens Council Polls to Coronation of Candidates' (The Guardian, 23 May 2024) https://guardian.ng/news/inec-knocks-siecs-likens-council-polls-to-coronation-of-candidates/ accessed 13 June 2026; Nick Dazang, 'Let SIECs Be' (Vanguard, 10 June 2024) https://www.vanguardngr.com/2024/06/let-siecs-be/ accessed 13 June 2026; Omolaoye, S. (2024) INEC knocks SIECs, likens council polls to coronation of candidates, The Guardian Nigeria, 23 May. Available at: https://guardian.ng/news/inec-knocks-siecs-likens-council-polls-to-coronation-of-candidates/ (Accessed: 13 June 2026); Itodo, S. (2024). Constitutional disempowerment of state electoral commissions and its impact on local government elections in Nigeria. Daily Trust / TheCable / Vanguard syndication. https://www.vanguardngr.com/2024/07/constitutional-disempowerment-of-state-electoral-commissions-and-its-impact-on-local-government-elections-in-nigeria.

44 Erunke, J. (2025) FOSIECON conference outlines measures to rebrand SIECs, Vanguard, 27 May. https://www.vanguardngr.com/2025/05/fosiecon-conference-outlines-measures-to-rebrand-siecs/; Leadership Newspaper (2025) FOSIECON conference outlines measures to rebrand SIECs, 27 May. https://leadership.ng/fosiecon-conference-outlines-measures-to-rebrand-siecs/; Eze, F. (2025) 2027: FOSIECON suggests ways to rebrand, strengthen SIECs, The Sun Nigeria, 27 May. https://thesun.ng/2027-fosiecon-suggests-ways-to-rebrand-strengthen-siecs/.

45 Section 30 NDPA.

46 Section 65 NDPA.

INEC collects the following biometric data during voter registration:

Biometric Type	Collection Method	Purpose
Fingerprint data	All ten digits scanned	Voter identification and duplicate detection
Facial recognition data	Digital photograph	Biometric verification via BVAS

The National Identity Management Commission (NIMC) similarly collects biometric data (fingerprints, facial images, digital signatures) for the National Identification Number (NIN). However, there is no current legal framework for integrating NIN biometric data with INEC's voter register, though interoperability remains a potential future development.[47]

2.3.3 Special Considerations for Sensitive Data Processing

Under section 30(1) of the Nigeria Data Protection Act (NDPA) 2023, the processing of sensitive personal data is generally prohibited, except where one of the statutory conditions permitting such processing is satisfied. These conditions include where the data subject has given explicit consent to the processing; where the processing is necessary for compliance with a legal obligation imposed on the data controller; where the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or where the processing is necessary to protect the vital interests of the data subject or another natural person.

For INEC, the primary lawful basis for biometric data processing is performance of a task carried out in the public interest (democratic elections) and compliance with a legal obligation (Electoral Act 2022 mandate to verify voter identity and prevent double voting). However, the NDPA also requires that processing of sensitive data be accompanied by a Data Protection Impact Assessment (DPIA) where processing is likely to result in high risk to data subjects' rights and freedoms.[48] Given that INEC processes biometric data of over 94 million citizens, a DPIA is statutorily required.

2.4 Voter Registration and Biometric Data Collection

2.4.1 The Voter Registration Process

Voter registration in Nigeria is a continuous process managed by INEC through the Continuous Voter Registration (CVR) system.[49] The registration process involves several sequential stages. First, an eligible citizen completes the registration form, either through physical registration or online pre-registration.

Next, the applicant undergoes document verification, where proof of identity such as a National Identification Number, international passport, or other approved identification is provided.

This is followed by biometric capture, during which all ten fingerprints and a facial image are recorded. The applicant's personal information is then entered into the Continuous Voter Registration (CVR) database. After successful registration, a Temporary Voter's Card (TVC) is issued, pending the production of the Permanent Voter's Card (PVC). Finally, the data is subjected to deduplication, where biometric matching is used to identify and eliminate any instances of multiple or duplicate registrations.[50] During the Anambra governorship election preparations, INEC uncovered 27,817 multiple registrations through biometric deduplication processes.[51]

2.4.2 Legal Framework for Biometric Data Processing

Biometric data in Nigeria is recognised under several laws and regulations, but there is no single, comprehensive framework specifically dedicated to it. From electoral perspective, the applicable legal instruments include:

Instrument	Relevance to Biometric Data
NDPA 2023	Classifies biometric data as sensitive; imposes enhanced protection requirements
NDPA General Application and Implementation Directive (GAID) 2025	Provides detailed guidance on sensitive data processing
Electoral Act 2022 (as amended 2026)	Mandates BVAS for voter verification, implying biometric processing
INEC Regulations and Guidelines	Specify biometric capture protocols

The NDPA has been critiqued for failing to provide a detailed definition of biometric data, creating ambiguity in interpretation.[52] The Act does not specify whether biometric data includes fingerprint data, facial recognition data, iris scanning data, voice recognition data, hand geometry data, DNA, or signature data. This ambiguity may affect how biometric data is regulated or litigated, particularly as new biometric technologies emerge.

2.4.3 Consent and Transparency Concerns

Biometric data collected by INEC is often mandatory for voter registration, meaning, citizens cannot register to vote without providing fingerprints and a facial image. This raises significant questions under the NDPA's consent framework.

Footnotes

47 Voice of Nigeria (2021) NIN not mandatory for voter registration – INEC, 2 April. https://von.gov.ng/nin-not-mandatory-for-voter-registration-inec/; The Cable (2025) Nigerians can register for NIN, voter cards at same centres, 4 Sept. https://www.thecable.ng/nigerians-can-register-for-nin-voter-cards-at-same-centres-says-inec/; Premium Times (2025) INEC, NIMC strengthen collaboration on citizens' registration' <https://www.premiumtimesng.com/news/more-news/818571-inec-nimc-strengthen-collaboration-on-citizens-registration-data-management.html; Independent Nigeria (2025) INEC, NIMC strengthen ties to streamline voter and identity registration, 3 Sept. https://independent.ng/inec-nimc-strengthen-ties-to-streamline-voter-identity-registration/

48 Section 28 NDPA.

49 Independent National Electoral Commission (INEC) – Guidelines for Registration (Official website)

https://www.inecnigeria.org/guidelines-for-registration/; Olumekun, S. (2025, August 7). All set for resumption of nationwide CVR Aug 18. INEC News < https://inecnews.com/all-set-for-resumption-of-nationwide-cvr-aug-18/> accessed 12 June 2026.

50 INEC Guidelines for Registration, https://www.inecnigeria.org/guidelines-for-registration/ /> accessed 12 June 2026.

51 Ripples Nigeria – INEC uncovers 27,817 multiple registrations in Anambra

https://www.ripplesnigeria.com/inec-uncovers-27817-multiple-registrations-in-anambra/; P.M. News – CVR: INEC uncovers 27,817 multiple registrations in Anambra

https://pmnewsnigeria.com/2025/09/05/cvr-inec-uncovers-27817-multiple-registrations-in-anambra/; The Eagle Online – INEC uncovers 27,817 multiple registrations in Anambra

https://theeagleonline.com.ng/inec-uncovers-27817-multiple-registrations-in-anambra-17-more-associations-seek-registration-as-parties/.

52 Idorenyin Ekpenyong, 'The Overlooked Risks of Deploying Biometric Data in Public Sector Databases in Nigeria: Balancing State Interests and Individual Rights in Data Management' (S.P.A. Ajibade & Co., 8 July 2025) https://webiis08.mondaq.com/nigeria/privacy-protection/1647526/ accessed 14 June 2026.

The collection of biometric data for voter registration under the CVR system raises two fundamental legal questions under Section 30(1) of the NDPA 2023. First, can consent be considered "explicit" and "freely given" when it is effectively coerced, where refusal to provide biometric data results in the denial of the right to vote? The absence of a meaningful alternative suggests that such consent may be invalid.

Second, does the mandatory collection of biometric data fall within the public interest exception, which would exempt INEC and SIECs from the requirement to obtain consent altogether? If the processing is deemed necessary for the performance of a task carried out in the public interest (specifically, the prevention of multiple registrations and electoral fraud) then electoral bodies may lawfully process sensitive biometric data without relying on consent as their legal basis. The interplay between these provisions remains unresolved and carries significant implications for data protection compliance at both national and state levels.

The better view is that INEC and SIECs rely on the public interest and legal obligation bases for processing biometric data under Section 30(1) of the NDPA 2023, not consent. First, Section 30(1) explicitly permits processing without consent where necessary for compliance with a legal obligation or for the performance of a task carried out in the public interest. Second, the right to vote is a constitutional right, and registration (including biometric capture) is a mandatory prerequisite for exercising that right. Third, biometric verification serves the compelling public interest of preventing electoral fraud, detecting multiple registrations, and ensuring the "one person, one vote" principle.[53] Consequently, electoral bodies process biometric data lawfully under the statutory exceptions to consent, and no conflict with the NDPA 2023 arises from mandatory biometric collection for voter registration.

However, even where consent is not required, the transparency obligations under Section 24(1)(a) and Article 7(m) GAID remain fully applicable. Voters must be clearly informed about what biometric data is collected, how it will be used, how long it will be stored, and with whom it may be shared.

2.4.4 Data Privacy Impact Assessment (DPIA) Requirement

Section 28 of the NDPA 2023 requires data controllers to conduct a DPIA where processing is likely to result in a high risk to data subjects' rights and freedoms.

The processing of biometric data of over 94 million citizens unquestionably meets this threshold. A DPIA for the INEC's voter registration system should comprehensively evaluate the nature and scope of the biometric data collected, including fingerprints, facial images, and other identifying information.[54]

The assessment should determine whether the processing of such data is necessary and proportionate to the objective of maintaining an accurate and credible voter register. It should also identify potential security risks, such as unauthorized access, data breaches, misuse of biometric information, and identity theft, and specify the technical and organizational measures required to mitigate those risks, including encryption, access controls, monitoring, and incident response procedures. In addition, the DPIA should assess how the system safeguards the rights of data subjects, ensuring that voters can exercise their rights of access, rectification, and erasure in accordance with applicable data protection laws.

The NDPC–INEC partnership, established in April 2026, which includes training on ISO 27701 Privacy Information Management System, suggests that such assessments are being prioritised.[55]

2.5 Digital Election Infrastructure and Data Ecosystems

2.5.1 Overview of Digital Election Systems

Nigeria's electoral process increasingly relies on a complex digital ecosystem comprising several interconnected systems. The Electoral Act 2026 (as amended) has reinforced this digital transformation by mandating electronic transmission of results and compulsory use of the Bimodal Voter Accreditation System (BVAS).[56]

Key Digital Election Systems:

System	Function	Data Processed
Continuous Voter Registration (CVR)	Online and physical voter registration	Personal data, biometrics
Bimodal Voter Accreditation System (BVAS)	Voter verification at polling units	Biometric data (fingerprint, facial)
INEC Result Viewing Portal (IReV)	Electronic transmission and viewing of results	Polling unit results, result sheets
Voter Register Database	Central repository of registered voters	All voter personal data
Political Party Digital Registers	Membership registers submitted to INEC	Party member personal data

Footnotes

53 Mudiaga-Odje, A. (2010, June 24). "One man, one vote", Electoral Act and the Constitution. Vanguard News. https://www.vanguardngr.com/2010/06/%E2%80%9Cone-man-one-vote%E2%80%9D-electoral-act-and-the-constitution/amp/> Accessed 9 June 2026; The Eagle Online. (2025, August 4). INEC appeals to voters reject double registration. https://theeagleonline.com.ng/inec-appeals-to-voters-reject-double-registration/> Accessed 9 June 2026.

54 The electoral bodies' (non)compliance with this, is discussed later in the study.

55 NDPC, INEC partner to protect voter data ahead of Nigeria's 2027 elections < https://www.itedgenews.africa/ndpc-inec-partner-to-protect-voter-data-ahead-of-nigerias-2027-elections/#mnmd-offcanvas-mobile> Accessed June 10, 2026; Technology Times, 'NDPC, INEC target data protection for 94m voters before 2027 elections' < https://technologytimes.ng/ndpc-inec-target-data-protection-for-94m-voters/?utm_source> Accessed June 10, 2026

56 Adeyemi A Adelowo, Olubukola F Alade, Bisi Olawunmi, Fadekemi N Adelowo and Peter A Obateru, 'Legislative Contingency and Electoral Transparency in Nigeria: Media Framing, the Electronic Transmission Provision and Public Trust under the Electoral Act 2026' (2026) 2(1) Impact International Journals and Publications 1609.

2.5.2 The Bimodal Voter Accreditation System (BVAS)

The BVAS is a handheld electronic device used by Presiding Officers to verify voters' identities at polling units through two biometric modalities - fingerprint and facial recognition - hence the designation 'bimodal'. Under section 47(2) of the Electoral Act 2026, a Presiding Officer is required to use a Bimodal Voter Accreditation System or any other technological device prescribed by the Commission for voter accreditation. Thus, while BVAS is expressly recognised as an accreditation technology under the Act, its use is not exclusive, as the Commission may prescribe an alternative technological device. Section 47(3) further provides for the cancellation and rescheduling of an election at an affected polling unit where the prescribed accreditation device fails, subject to the conditions stipulated in the provision.[57]

2.5.3 Data Flow in BVAS Operations:

The BVAs operates through a structured electoral data workflow that begins in the pre-election phase, where devices are configured with voter registers specific to designated polling units. During accreditation, voters present themselves at polling units and are verified through fingerprint scanning or facial recognition, with biometric inputs matched against the INEC voter database to confirm eligibility and prevent multiple registration or impersonation. Once accreditation is successful, the voter proceeds to cast their ballot, noting that BVAS does not capture or record voting preferences. After voting, the device is also used to capture and transmit polling unit results to the INEC Results Viewing Portal (IReV). Because BVAS processes sensitive biometric information at the point of accreditation, it generates significant data protection obligations, including the need to secure devices against theft, tampering, or unauthorised access, ensure data minimisation by limiting stored biometric information to what is strictly necessary for authentication, and implement post-election data deletion protocols to prevent unlawful retention or secondary use of voter data.

The adequacy of these safeguards, however, cannot be assessed solely by reference to the formal architecture of BVAS. The more important question is whether the obligations of security, minimisation, restricted access and appropriate retention have been effectively implemented in practice. This is particularly important because BVAS represents a significant concentration of biometric and electoral information in a relatively small number of technological systems.

The evolution from the Smart Card Reader to BVAS was partly a response to earlier operational problems, including failures to read voter cards and fingerprints, bypassing of accreditation procedures and the use of other persons' voter cards.[58] The Commission's post-election review of the 2023 General Election[59] also records that, unlike the earlier Smart Card Reader, the voters' register was resident on the BVAS device. The migration of voter information onto the accreditation device therefore improves authentication but simultaneously makes the security of the device, its software, local storage and transmission channels an important component of voter privacy protection.

There are also indications that the data-protection governance surrounding electoral technology is still developing. In April 2026, the NDPC and INEC established a joint working group specifically to strengthen the integration of data protection and privacy into Nigeria's electoral system. The NDPC noted that INEC holds the personal data of approximately 94 million Nigerians and identified the need to strengthen safeguards for voter information and responsible processing by third parties and vendors. The establishment of this working group is significant: it demonstrates institutional recognition of the scale of the privacy risk, but it also suggests that the integration of data-protection governance into electoral administration remains an evolving process rather than a settled compliance achievement.

The principal difficulty, therefore, is not necessarily establishing whether BVAS has a legitimate electoral purpose. Its purpose in verifying voter identity and preventing impersonation is readily apparent. The difficulty lies in demonstrating that every stage of the resulting data lifecycle is adequately governed. A data-protection assessment must extend beyond the moment of biometric authentication to encompass the collection, temporary storage, transmission, access, maintenance, retention and eventual deletion or secure disposal of the information.[60] INEC's current biometric registration privacy notice, for example, expressly identifies fingerprints, facial images or templates and other biometric identifiers as information that may be processed and states that such information is used for biometric enrolment, identity verification, preventing duplicate or fraudulent registrations and maintaining the integrity of the National Register of Voters. The critical question is whether equivalent specificity exists in relation to BVAS operations, including the precise retention periods applicable to biometric information captured or accessed during accreditation, the circumstances in which information is transferred from devices to central systems, the persons authorised to access it, and the mechanisms for its deletion or secure disposal.

Footnotes

57 Ugar, A. A., Edino, O. F., Agbor, U. I., & Nwagboso, C. I. (2024) Elections Administration and Bimodal Voter Accreditation System (BVAS) Technology. International Journal of Public Administration in the Digital Age, 11(1), 1–31. https://doi.org/10.4018/IJPADA.352042; Onu, F. U., Ezea, I. J., Egbono, F., & Ogbaga, I. (2023). The Bimodal Voter Accreditation System (BVAS) in 21st Century Nigeria Election: Security Breaches and Solutions. IOSR Journal of Computer Engineering, 25(4), 22–26. https://doi.org/10.9790/0661-2504012226; Ogbadebo, A. (2025). The Role of BVAS in Safeguarding Electoral Integrity: An Evaluation of the 2023 General Elections in FCT, Abuja. Journal of Social Political Sciences, 6(1). https://doi.org/10.52166/jsps.v6i1.25;

58 Kassem, Semshak Danladi and Shakira Hannah Osasona, 'Smart Card Reader and Election Credibility in Nigeria's Fourth Republic' (2021) 2(2) Zamfara Journal of Politics and Development

59 The Report has now been taken down from the Commission's website.

60 Habiba Musa, 'Data Protection Issues in the Management of the Bimodal Voters Accreditation System (BVAS) in Nigeria' (2023) 10(2) Nnamdi Azikiwe University Journal of Commercial and Property Law.

The consequences of inadequate compliance are considerable. Unlike passwords or identification numbers, biometric characteristics cannot ordinarily be replaced once compromised. Unauthorised access to fingerprints or facial biometric information may therefore create a persistent risk of identity fraud, impersonation, surveillance and other forms of misuse. A compromise of electoral data may also reveal information capable of linking individuals to particular polling locations or electoral records.[61] More broadly, a breach involving millions of voters could undermine public confidence not only in INEC's data-management practices but also in the integrity and legitimacy of the electoral process itself. The risks are consequently both individual and systemic: the individual voter may suffer privacy and identity-related harm, while the electoral system may suffer loss of public trust.[62]

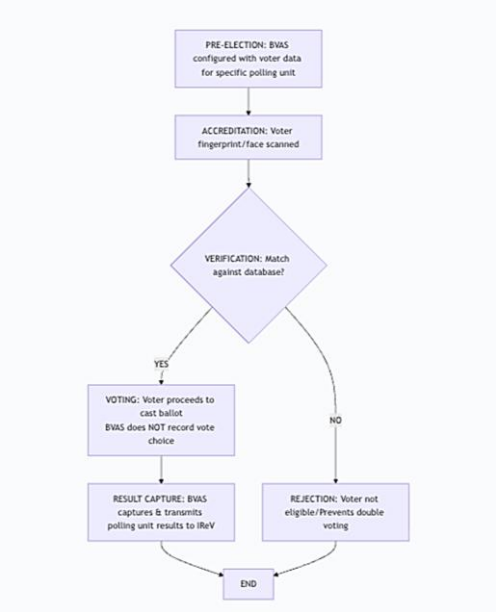
The experience of the 2023 elections demonstrates why technological effectiveness and data-protection compliance must be assessed separately. BVAS was introduced to address weaknesses associated with previous accreditation technology and INEC reported substantial improvements in accreditation performance. However, the successful achievement of an electoral objective does not, by itself, establish compliance with data-protection principles. An electoral technology may be effective in preventing impersonation while simultaneously creating risks relating to excessive collection, inadequate security, uncontrolled access or excessive retention. Data protection therefore requires an assessment not merely of whether the technology works, but of how the personal data enabling it to work is governed throughout its lifecycle.[63]

International practice supports this lifecycle-based approach. The Council of Europe has specifically identified voter registration and authentication as areas requiring heightened protection, particularly where biometric information is used. Its guidance emphasises lawful processing, transparency, data security, data-subject rights and safeguards appropriate to the risks created by biometric voter identification systems.[64] Similarly, the United Kingdom's Electoral Commission's data-protection guidance requires electoral officials to apply data minimisation, secure storage, appropriate retention and secure disposal, emphasising that personal data should not be retained longer than necessary for the purpose for which it was collected.[65] These practices suggest that electoral bodies should maintain documented retention schedules, access controls, audit trails and secure disposal procedures rather than treating election-day processing as an isolated activity. A further international benchmark is the requirement for transparency concerning biometric processing.

The American National Institute of Standards and Technology's current digital identity guidance recommends that organisations using biometrics provide publicly available information explaining what biometric information is collected, how it is stored and protected, and how it may be removed in accordance with applicable law.[66] It also recommends a documented and publicly available deletion process and default retention period for biometric information. Although these standards are not directly binding on INEC, they provide a useful benchmark against which Nigerian electoral practice can be evaluated.

Accordingly, the assessment of BVAS should not be limited to asking whether biometric verification occurs lawfully. It should examine whether INEC can demonstrate, through policies, technical controls, audit records, retention schedules, contractual arrangements and other documentary evidence, that biometric information is protected throughout its lifecycle. Particular attention should be paid to whether biometric data remains on BVAS devices after accreditation, how devices are secured before and after polling, how data is transmitted and encrypted, who can access the information, whether third-party vendors have access to it, whether access is logged and audited, and what happens to the data once the electoral purpose has been fulfilled.

The central issue is therefore one of accountability. The existence of BVAS privacy safeguards on paper is not sufficient. INEC should be able to demonstrate that the safeguards operate effectively in practice and that the processing of biometric voter information is limited to what is necessary for legitimate electoral purposes. This distinction between formal compliance and demonstrable compliance is critical to determining the actual level of voter privacy protection under Nigeria's data-protection framework.[67]



Footnotes

61 Carra Pope, 'Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protecting Biometric Data' (2018) 26 Journal of Law and Policy 769.

62 Alexander Boniface Makulilo, 'Rebooting Democracy? Political Data Mining and Biometric Voter Registration in Africa' (2017) 26(2) Information & Communications Technology Law 198–212.

63 Toba Paul Ayeni and Opani Meshark Aweh, 'Examining the Impact of Bimodal Voter Accreditation System (BVAS) as a Gamechanger in Nigeria 2023 Elections' (2024) 20(2) The Information Technologist 25–42.

64 Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Guidelines on the Protection of Individuals with regard to the Processing of Personal Data for the Purposes of Voter Registration and Authentication (Council of Europe 2024) paras 4.6–4.7.

65 Electoral Commission, Data Protection Guidance for Electoral Registration Officers and Returning Officers (Electoral Commission, updated 15 May 2025) https://www.electoralcommission.org.uk/full-guidance/data-protection-guidance-electoral-registration-officers-and-returning-officers accessed 12 September 2026.

66 National Institute of Standards and Technology, Digital Identity Guidelines: Identity Proofing and Enrollment (NIST Special Publication 800-63A-4, 2025) § 3.1.11.

67 The NDPC's 2023 Annual Report reinforces this approach by describing Compliance Audit Returns as a "potent tool of accountability" and identifying documentation of compliance and data-processing activities as audit parameters. Nigeria Data Protection Commission, Nigeria Data Protection Annual Report 2023 (2024) 23, s 4.3 'NDPA Compliance Audit Returns'.

2.5.4 INEC Result Viewing Portal (IReV)

The IReV portal facilitates the electronic transmission and public viewing of polling-unit results, enabling citizens, political parties and electoral observers to access results as they are uploaded. Under section 60(3) of the Electoral Act 2026, Presiding Officers are required to electronically transmit the results of the poll to the IReV portal. Where such transmission fails due to communication failure, however, the Act preserves Form EC8A as the primary source for the collation of results. The statutory duty is reinforced by section 60(6), which provides that any person who wilfully contravenes section 60 is liable to a fine of not less than ₦500,000 or imprisonment for a term of not less than six months, or both. Thus, the statutory sanction attaches to wilful contravention of the results-transmission requirements under section 60 generally, rather than exclusively to the failure to upload results to IReV.[68]

2.5.5 Data Protection Implications of IReV:

The IReV raises distinct data protection considerations because it involves the public disclosure of electoral data, creating a tension between transparency and privacy.[69] While the platform is designed to enhance electoral transparency, there is a risk that, if proper safeguards are not implemented, it could inadvertently expose personal voting-related information that ought to remain confidential through inadequate anonymisation.[70]

The safeguards should not be understood as measures that undermine IReV's transparency objective. Rather, they should ensure that transparency is achieved without exposing more personal information than is necessary to verify electoral results. First, INEC should apply data minimisation and effective anonymisation or redaction to information published through IReV. Information necessary to verify a polling-unit result, such as the polling-unit identifier, votes recorded for each candidate, rejected ballots and the relevant result sheet, may legitimately be made available to the public. By contrast, individual biometric identifiers, voter identification numbers, addresses, telephone numbers and other information capable of identifying particular voters should not be publicly disclosed unless demonstrably necessary for a specific and lawful electoral purpose. Anonymisation should also be sufficiently robust to prevent re-identification through the combination of information appearing on the result sheet with other publicly available electoral information.[71]

Secondly, technical and organisational safeguards should preserve the separation between voter identity and electoral results. The transparency function of IReV should enable the public to establish what occurred at a polling unit without enabling the public to determine which particular individual was accredited or how that individual voted. This requires appropriate access controls, encryption, secure transmission, role-based permissions and audit trails governing access to the underlying electoral databases and BVAS-generated information. Public access to IReV should not therefore operate as indirect access to the underlying voter-registration or biometric database.[72] INEC should also maintain auditable records identifying who accessed, uploaded, altered or otherwise processed electoral information, so that unauthorised access can be detected and investigated. These safeguards are particularly important because the disclosure of electoral information can create risks not only through direct identification but also through linkage and inference, especially where information concerning a small polling unit is combined with other publicly accessible information.

Thirdly, retention and deletion controls are necessary to prevent transparency from becoming indefinite public exposure. INEC should establish and publicly communicate the categories of information retained through IReV and associated electoral systems, the purpose and legal basis for retention, the applicable retention periods, the persons authorised to access retained information, and the circumstances in which information is archived, anonymised or securely deleted. The fact that information has legitimately been made available for electoral verification does not necessarily justify its indefinite retention or continued public accessibility. The appropriate standard should therefore be one of privacy-preserving transparency. IReV should provide sufficient information to facilitate meaningful electoral scrutiny and verification while limiting the collection, disclosure, accessibility and retention of personal information to what is necessary and proportionate for legitimate electoral purposes. This approach gives practical effect to data minimisation, purpose limitation, storage limitation, integrity and confidentiality, and accountability under Nigeria's data-protection framework.[73]

In addition, uploaded result sheets may contain handwritten entries, signatures, or other identifying marks of polling officials, which could constitute personal data and therefore require appropriate handling under data protection principles. Furthermore, concerns around data accuracy arise, as errors during transmission or uploading could lead to the publication of incorrect results, potentially undermining public trust in the electoral process and the integrity of the system.[74]

2.5.6 The National Voter Register

INEC maintains a centralised National Voter Register containing the personal and biometric data of all registered voters.

Footnotes

68 Section 60, Electoral Act 2026.

69 Oluwaseun Clement Ajayi, Abraham Musa Peter and Margaret Apine, 'An Assessment of the Impact of Technological Innovations on Electoral Credibility in Nigeria, 2015–2023' (2026) 4(1) International Journal of Education, Culture, and Society 146 https://doi.org/10.58578/ijecs.v4i1.8405

70 Femi Samuel Oladele, 'Technology Security and Electoral Credibility in Nigeria: A National Security Review of BVAS and IReV in the 2023 General Elections' (2025) 8(3) International Journal of Intellectual Discourse.

71 Article 26(2)(b), GAID 2025 expressly requires controllers relying on legitimate interest to "prioritise privacy by design and by default", taking into consideration the "suitability of anonymisation or pseudonymisation."

72 See section 24 of the NDPA.

73 INEC's own privacy policy is particularly useful because it recognises retention limitation, secure deletion, anonymisation/archiving, access controls and accountability as elements of its data-protection framework. Although the policy should not automatically be treated as governing every aspect of IReV, it provides useful evidence of the safeguards that INEC itself recognises as appropriate for its processing activities. See Independent National Electoral Commission (INEC), 'Privacy Policy' (effective 16 March 2024) https://www.inecnigeria.org/privacy-policy/ accessed 12 September 2026.

74 Olasupo O Thompson, Ridwan Tosho Idris, Olugbenga Seun Aina, James Sanmi Adekola and Surajudeen Oladotun Oladele, 'Digital Electoral Reforms and Democratic Consolidation: A Critical Assessment of BVAS and IReV in the 2023 Nigerian General Elections' (2025) 8(2) Gusau International Journal of Management and Social Sciences https://doi.org/10.57233/gijmss.v8i2.1; Ugo Chuks Okolie, 'BVAS, IReV and Democratic Elections in Nigeria' (2024) 2(3) Pinisi Journal of Social Science https://doi.org/10.26858/pjss.v2i3.5871; Oluwaseun Clement Ajayi and Olumorin O M, 'Technological Innovations and the Outcomes of the 2023 General Elections in Nigeria' (2025) African Journal of Democracy and Election Research;Adelowo AA et al, 'Legislative Contingency and Electoral Transparency in Nigeria: Media Framing, Electronic Transmission Provision and Public Trust under the Electoral Act 2026' (2026) Impact International Journals and Publications.

This database, often referred to as holding over 94 million records, is a critical national asset but also a significant data protection risk.[75]

The risk arises from the scale, sensitivity and centralisation of the information held by INEC. A centralised voter register does not merely contain ordinary identifying information; it may contain information capable of uniquely distinguishing individuals, including biometric identifiers used for voter authentication. The concentration of such information creates a valuable target for unauthorised access, cyberattacks, insider misuse, unlawful disclosure and secondary use. The consequences of compromise are particularly serious in the electoral context because biometric characteristics are inherently persistent: unlike passwords or identification numbers, fingerprints and facial characteristics cannot ordinarily be replaced once compromised.[76] Centralisation may also facilitate the aggregation and linkage of voter information with other databases, creating risks of profiling, surveillance, discrimination or other forms of misuse beyond the immediate purpose of voter registration and authentication. The scale of the register consequently magnifies the consequences of any failure in security, access control, retention or governance. INEC's position as custodian of a database containing information relating to millions of voters therefore makes data minimisation, strict purpose limitation, robust technical and organisational security, controlled access, retention limits, auditability and demonstrable accountability particularly important under the Nigeria Data Protection Act 2023. As Makulilo observes in the African electoral context, biometric voter registration involves "massive political data mining" and presents significant personal-information protection challenges.[77]

2.5.7 Security Requirements for the Voter Register:

Requirement	NDPA Basis	Current Status
Access controls	Section 24(1)(f) (integrity and confidentiality)	Under NDPC–INEC partnership
Encryption	Section 24(1)(f)	Not publicly confirmed
Audit logging	Accountability principle Section 24(3)	INEC has audit trail capabilities
Data breach notification	Section 40	Under development
Third-party access restrictions	Section 24(1)(a) (fairness and transparency)	Addressed by NDTC-NDPC partnership

2.6 Third-Party Data Sharing and Technology Vendors

2.6.1 The Data Processing Ecosystem

INEC's electoral operations involve numerous third-party relationships that implicate data protection obligations. INEC's electoral operations involve numerous third-party relationships that implicate data protection obligations. In the course of voter registration, voter accreditation, election administration and the management of electoral databases, INEC may engage technology vendors, biometric solution providers, software developers, data-hosting and cloud-service providers, telecommunications operators, logistics companies, printing contractors, security agencies and other public or private entities that may have access to, process, transmit or otherwise handle voters' personal data.[78]

These relationships are particularly significant because the involvement of a third party does not, by itself, displace INEC's obligations as a data controller under the NDPA.[79] Rather, INEC must ensure that personal data entrusted to processors and other third parties is processed only for legitimate and specified purposes, subject to appropriate contractual, organisational and technical safeguards. The risks are heightened where third parties obtain access to sensitive electoral information, including biometric and identification data, because unauthorised disclosure, loss, alteration, secondary use or inadequate security at any point in the processing chain may compromise voter privacy and electoral integrity. Consequently, an assessment of INEC's compliance with the NDPA must extend beyond its internal data-processing practices to examine the manner in which it selects, contracts with, supervises and monitors third parties involved in the electoral data ecosystem. The NDPC–INEC partnership explicitly recognises the need to extend compliance oversight to third-party vendors.[80]

2.6.2 Categories of Third-Party Data Processors:

Vendor/ Partner Category	Role	Data Access	NDPA Status
Technology Providers	BVAS hardware and software, CVR platform	Voter data, biometrics	Data processors under Section 65
Cloud Service Providers	Data storage, backup	Voter data	Data processors
Election Observers	Limited access for monitoring	Aggregated or anonymised data	Third-party recipients
Political Parties	Receive copies of voter register (limited)	Voter names, addresses	Data controllers (independent)
Security Agencies	Election security	Limited operational data	Competent authority exemptions possible

Footnotes

75 Independent National Electoral Commission, 'Preliminary Voters' Register Hits 93.52 Million, INEC Insists on BVAS, IReV for 2023 Polls' (26 October 2022) https://inecnews.com/voters-register-hits-93-52m-inec-insists-on-bvas-irev-for-2023-polls/ accessed 15 June 2026.

76 Jack Cable, et al 'A Systematization of Voter Registration Security' (2023) 9(1) Journal of Cybersecurity tyad008.

77 Alexander Boniface Makulilo, 'Rebooting Democracy? Political Data Mining and Biometric Voter Registration in Africa' (2017) 26(2) Information & Communications Technology Law 198–212.

78 Independent National Electoral Commission, 'Privacy Policy, Terms & Conditions' (Personal Biometric Registration Application, 1 July 2026) https://cvr.inecnigeria.org/legal accessed 12 September 2026.

79 Section 29 NDPA imposes obligations on data processors (third party vendors), including the requirement to implement appropriate technical and organisational measures to ensure the security, integrity and confidentiality of personal data. It also requires the relationship between controller and processor to be governed by a written agreement.

80 Ibid.

2.6.3 Data Processor Obligations Under the NDPA

Under section 29 of the NDPA, data controllers such as INEC and SIECs remain accountable for ensuring that any data processors (vendors) engaged on their behalf comply with the requirements of the Act. This obligation extends to third-party vendors involved in the collection, storage, transmission, or processing of electoral data. Consequently, the electoral bodies are expected to establish formal data processing agreements that clearly define the processor's data protection responsibilities and ensure compliance with applicable legal standards.

They must also conduct periodic security assessments and audits to evaluate the adequacy of vendors' technical and organisational measures for protecting personal data. In addition, the vendors should not engage sub-processors without the prior authorisation of the electoral bodies, thereby enabling effective oversight of the entire processing chain. Where a personal data breach occurs, vendors are required to promptly notify the electoral bodies to facilitate timely reporting, mitigation, and compliance with statutory breach-notification obligations.[81] The partnership between the NDPC and INEC seeks to reinforce these accountability and oversight mechanisms, particularly in relation to third-party vendors and other entities involved in processing voter data within Nigeria's electoral ecosystem.[82]

2.6.4 NDPC–INEC Partnership and Vendor Accountability

The NDPC–INEC partnership should not, in itself, be regarded as the source of legally enforceable obligations owed by electoral vendors. The primary obligations governing INEC's engagement of data processors arise from the NDPA which requires a controller engaging a processor to ensure compliance with applicable data-protection obligations and requires the processing relationship to be governed by a written agreement.[83] The Act further imposes security obligations on processors and requires a processor that becomes aware of a personal-data breach to notify the controller or processor that engaged it.[84]

Consequently, the partnership is better understood as an institutional and regulatory mechanism for facilitating compliance, coordination, supervision and capacity building rather than as legislation creating new substantive duties.[85] Unless the particular instrument establishing the partnership contains independently enforceable contractual undertakings, its provisions are more appropriately characterised as a form of regulatory soft law. Its significance therefore lies not in creating obligations that did not previously exist, but in providing an institutional framework through which the obligations already imposed by the NDPA can be implemented and monitored within the electoral ecosystem.

The legal force of the NDPA, however, can be reinforced through the contractual relationship between INEC and its vendors. A data-processing agreement executed pursuant to section 29 is capable of creating directly enforceable contractual obligations concerning confidentiality, security, permitted processing, breach notification, audit rights, data retention and deletion, and restrictions on further processing.[86] The GAID strengthens this approach by expressly contemplating written contracts, data-processing agreements, ongoing processor monitoring, due diligence, security of storage and transfers, processor participation in DPIAs and incident-response protocols. Thus, while the NDPC–INEC partnership may itself constitute soft law, a requirement emerging from the partnership and incorporated into a binding procurement contract or data-processing agreement may acquire contractual force. The distinction is particularly important for a doctrinal study. Hence, evidence that INEC participates in a regulatory partnership should not automatically be treated as evidence of legal compliance; rather, only where the partnership has translated into enforceable contractual controls and demonstrable oversight of the vendors processing electoral data.

Whether the NDPA framework constitutes global best practice requires a more critical assessment. The Act provides a substantial foundation for processor accountability: it requires written arrangements, imposes security obligations, requires risk-sensitive technical and organisational measures and provides for processor notification of data breaches. The GAID further operationalises these requirements by expressly asking organisations whether they monitor processor compliance, conduct due diligence, verify relevant certifications or standards, secure methods of storage and transfer, involve processors in DPIAs and maintain incident-response protocols. Nevertheless, the Nigerian framework does not reproduce all of the safeguards found in more mature international frameworks. For example, article 28(2) of the EU GDPR expressly prohibits a processor from engaging another processor without the controller's prior specific or general written authorisation, while article 28(3)(h) expressly requires processors to provide information necessary to demonstrate compliance and to allow and contribute to audits and inspections.[87] By contrast, section 29 of the NDPA requires notification when a new processor is engaged but does not formulate the same express prior-authorisation requirement for sub-processors.

Footnotes

81 Section 40(1)(a) NDPA.

82 Ibid.

83 Section 29(2) further provides that these measures include a written agreement between the controller and processor.

84 Section 39(1) NDPA.

85 National Data Protection Commission, 'Securing 94 Million Identities: NDPC and INEC Form Strategic Pact to Safeguard Voter Privacy' (15 April 2026)

86 Piotr Brzeziński, 'Personal Data Processing Contract' (2019) 13(4) Ius Novum 184, 184–195

87 Christopher Millard and Dimitra Kamarinou, 'Article 28. Processor' in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), The EU General Data Protection Regulation (GDPR): A Commentary (OUP 2020) 599–611.

This is significant in the electoral context because a chain of vendors can create a corresponding chain of risks, potentially extending processing beyond the electoral body's effective visibility and control.[88]

Accordingly, the NDPA should be regarded as providing a substantial but not exhaustive foundation for global best practice in electoral vendor governance. The principal gap is not necessarily the absence of a general legal obligation to protect personal data, but the absence of sufficiently prescriptive statutory requirements concerning the continuous governance of complex processor and sub-processor chains.[89] For electoral bodies processing large volumes of identification and biometric information, best practice would require more than the execution of a DPA at the commencement of a vendor relationship.

It should encompass documented vendor due diligence, risk classification, periodic independent security assessments, express audit and inspection rights, prior authorisation or effective objection rights regarding sub-processors, maintenance of an up-to-date processor register, mandatory breach-escalation procedures, verification of compliance throughout the processing lifecycle, and secure deletion or return of electoral data upon termination.[90] The NDPC–INEC partnership could therefore play an important role in closing this implementation gap, but its success should ultimately be measured by whether it produces such verifiable controls rather than merely by the existence of the partnership itself. In this sense, the partnership represents an opportunity to transform the NDPA's general statutory principles into a more robust and auditable system of electoral-data governance.

Footnotes

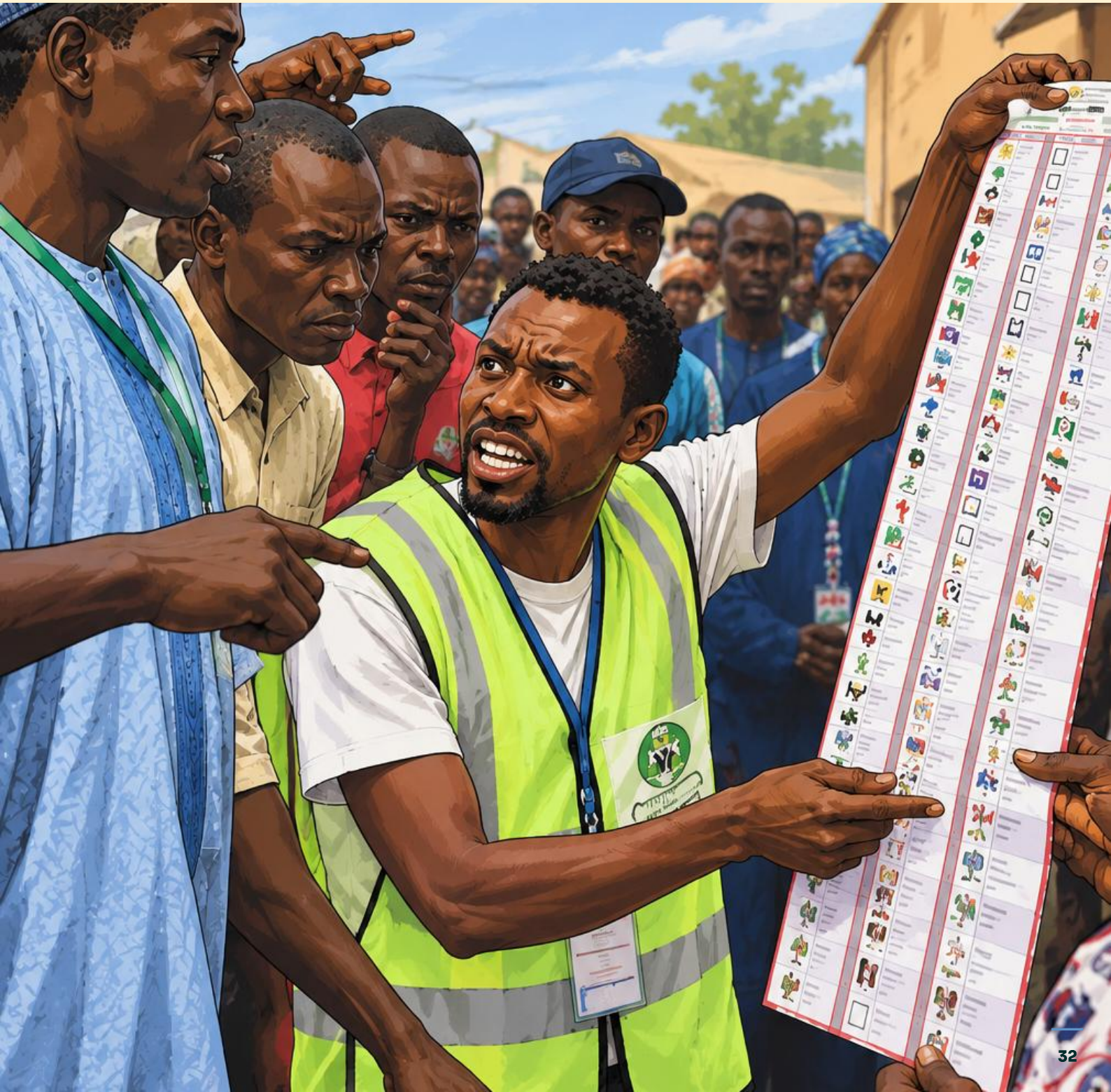
88 René Mahieu, Joris van Hoboken and Hadi Asghari, 'Responsibility for Data Protection in a Networked World: On the Question of the Controller, "Effective and Complete Protection" and its Application to Data Access Rights in Europe' (2019) 10 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 85, 87.

89 René Mahieu, Joris van Hoboken and Hadi Asghari, 'Responsibility for Data Protection in a Networked World: On the Question of the Controller, "Effective and Complete Protection" and its Application to Data Access Rights in Europe' (2019) 10 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 85, 87.

90 David Bomhard and others, 'Cybersecurity in Outsourcing and Cloud Computing: A Growing Challenge for Contract Drafting' (2021) 2 International Cybersecurity Law Review 147.

CHAPTER 3
ASSESSMENT OF COMPLIANCE WITH THE NDPA 2023

VOTER PRIVACY AND UMPIRES' TRANSPARENCY: AN ASSESSMENT OF THE ELECTORAL BODIES' COMPLIANCE WITH THE NIGERIA DATA PROTECTION ACT (NDPA) 2023



3.1 Transparency and Privacy Notice Compliance

Transparency is a foundational principle of data protection law, requiring data controllers to provide data subjects with clear, accessible information about how their personal data is collected, processed, stored, and shared.[91] Under the NDPA 2023, transparency obligations are articulated in Section 24(1)(a) and amplified under article 42(2) GAID.

3.1.1 Legal Framework for Transparency

Article 7(k) of the GAID prescribes specific requirements for transparency. To comply with the provisions of the NDP Act, electoral bodies and their vendors are required, among other obligations, to publish their organisational privacy policies on their platforms to inform the electorate about their data processing activities, as well as their rights and obligations in relation to such processing. In addition, the electoral bodies and their vendors must provide privacy and cookie notices on the homepage of their websites.[92] The cookie notice must afford data subjects a clear opportunity to accept or decline the use of cookies.[93] It should be displayed prominently in a manner that draws the attention of users, including by appearing in the centre, left or right section of the homepage. Displaying a cookie notice only at the bottom of a webpage, where it is likely to be overlooked or ignored by data subjects, undermines the principle of transparency in data processing.[94]

3.1.2 The Findings: Widespread Non-Compliance

This study interrogates the compliance of Nigeria's electoral bodies (INEC and SIECs) with their data transparency obligations under the NDPA, especially on their respective websites (where available). Given the centrality of voter data to the integrity and credibility of electoral processes, our study evaluates the extent to which these institutions have discharged their duties to inform citizens about the collection, use, and storage of their personal information, to provide mechanisms for data subjects to exercise their rights, and to maintain transparent and accountable data processing practices. The findings of this investigation, which we present below, paint a troubling picture of systemic non-compliance that not only undermines the constitutional right to privacy but also threatens to erode public trust in the electoral process itself, highlighting the urgent need for regulatory intervention and institutional reform.

3.1.3 INEC's Website Non-Compliance

A review of the official website of INEC revealed that, as of 1 June 2026, when this study commenced, the Commission did not provide a readily accessible privacy notice specifically addressing the processing of personal data through its public-facing website.[95] Earlier reports had similarly identified deficiencies in INEC's online privacy transparency.[96] This finding is significant, but it should not be understood as establishing, without more, that INEC had failed to comply with its transparency obligations in respect of the personal data contained in the national voter register. The principal processing of voters' biometric and demographic information occurs through electoral registration and other dedicated electoral systems and processes, rather than necessarily through INEC's general website. Accordingly, section 27 of the NDPA should be assessed by reference to whether INEC provides the prescribed information to data subjects at the point, or in connection with the process, through which their personal data are collected or otherwise obtained. The absence of a privacy notice on the general website is therefore not, standing alone, conclusive evidence of a failure to comply with section 27 in relation to the processing of the voter register.

Users may provide personal information when making enquiries, submitting complaints or requests, applying for employment or interacting with other online services, while technical information may also be generated through their use of the website. The appropriate inquiry is therefore whether INEC provides such website users with the information required by section 27 concerning the identity of the controller, purposes and lawful basis of processing, recipients, retention, data-subject rights and available avenues for complaints. More importantly, the website can serve as an accessible supplementary transparency mechanism through which INEC communicates its broader data-protection practices, including the processing of voter information, provided that such general notice does not substitute for the specific information that must be supplied to voters at the point of electoral-data collection. The significance of the website finding consequently lies not in demonstrating that the absence of a website notice automatically invalidates INEC's processing of voter data, but in identifying a potential deficiency in INEC's digital transparency architecture and prompting further examination of whether appropriate privacy information is provided across the distinct stages of the electoral-data lifecycle.

Nevertheless, INEC's website constitutes the natural and primary point of reference for any inquiry into the Commission's privacy and data-processing practices. As the principal public-facing digital platform of the electoral body, it is reasonably expected to provide accessible information concerning how INEC collects, uses, shares, retains and protects personal data.[97]

Footnotes

91 Emmanuel Okpara et al, 'The Foundation of Data Protection: Exploring Nigeria's Key Principles' (2025) Nigerian Journals Online.

92 Article 7(k) GAID.

93 Article 19, GAID.

94 Benjamin Maximilian Berens and others, 'Cookie Disclaimers: Dark Patterns and Lack of Transparency' (2024) 136 Computers & Security 103507.

95 https://wp1.inecnigeria.org/ Accessed 22 June 2026. The Electoral Act 2022 expressly contemplates and requires INEC to use an official website for the discharge of specified statutory functions. For instance, section 19(1) requires the Commission to publish or display copies of the voters' register for public scrutiny at every registration area and on its official website, or on any website established by the Commission for that purpose. Similarly, section 68 requires the Commission to publish on its website specified information concerning candidates and election results. These provisions demonstrate that the legislature has incorporated INEC's website into the statutory architecture of electoral transparency. Accordingly, while the Act does not appear to contain a standalone provision phrased as a general duty to "maintain a website", the statutory requirement to perform specified functions through an official website necessarily presupposes the existence and continued availability of such an online platform.

96 See Foundation for Investigative Journalism, 'NPF, INEC, JTB, NAFDAC Collect Personal Data Only to Disregard Privacy Policies' < https://fij.ng/article/npf-inec-jtb-nafdac-collect-personal-data-only-to-disregard-privacy-policies/> Accessed June 22, 2026; Timi Olagunju, 'How INEC and Nigeria's Major Parties Are Failing the First Test of Digital Democracy' < https://www.techpolicy.press/how-inec-and-nigerias-major-parties-are-failing-the-first-test-of-digital-democracy/> Accessed 22 June 2026.

97 Section 27 NDPA 2023.

The absence of a readily accessible privacy notice on the website therefore raises a legitimate transparency concern, particularly because data subjects should not be required to navigate disparate electoral processes or make separate inquiries merely to ascertain the Commission's general data-protection practices. While the website notice cannot substitute for the specific information that must be provided to data subjects at the point of collection under section 27 of the NDPA, its absence nevertheless impairs the accessibility and effectiveness of INEC's broader transparency framework. The failure to discharge this fundamental obligation constitutes a blatant violation of the Act and represents a stark failure of transparency and accountability on the part of the Commission. This finding, which is substantiated by the review of the Commission's website, raises serious questions about INEC's commitment to safeguarding the privacy rights of Nigerian citizens and to some extent, credibility of the electoral process.

However, when proceedings were commenced against INEC concerning the absence of a privacy policy on its website,[98] the Commission subsequently published a privacy policy. A review of that policy reveals an important limitation. The policy is principally directed at INEC's website-related processing activities, including forms, cookies, enquiries and recruitment, but contains little or no information concerning the Commission's core electoral-data processing activities, particularly voter registration and biometric capture. This omission requires careful qualification. Section 27(3) of the NDPA requires the information specified in section 27(1) to be contained in a privacy policy and expressed in a clear, concise, transparent, intelligible and easily accessible format, having regard to the class of data subjects targeted by the processing. The provision does not necessarily require every aspect of INEC's processing activities to be reproduced on its general website. Nevertheless, where INEC processes the biometric and demographic data of voters, the relevant data subjects must be provided with the information prescribed by section 27 in an accessible privacy policy or equivalent notice appropriate to the processing in question.

The GAID reinforces this contextual approach. Article 7(k) requires organisational privacy policies to be published on the controller's platforms, Article 7(l) specifically requires a privacy and cookie notice on the homepage of the website, while Article 7(m) requires privacy information to be transparently and appropriately provided on the platforms or places where processing occurs. The legal question is therefore not simply whether INEC's website policy describes biometric processing that does not take place on the website, but whether voters are provided with clear and accessible privacy information when their personal data are collected and processed through voter-registration and biometric-enrolment processes. Given that biometric data constitute a particularly sensitive category of personal data under the NDPA, the adequacy of the information supplied at those points assumes heightened significance. Accordingly, the study's finding should be framed as a transparency concern requiring further examination of INEC's privacy notices across its different processing environments, rather than as a categorical conclusion that the website policy itself is unlawful merely because it does not describe processing that occurs outside the website.

Also, INEC, as a public authority that processes the personal data of millions of Nigerians, is undoubtedly a controller of major importance, hence it is under a mandatory obligation to designate a Data Protection Officer (DPO).[99] Article 11(2) of GAID provides that: "The data controller or the data processor shall publish the contact details of the DPO and communicate the same to the Commission in the prescribed form." Contrary to this mandatory requirement, INEC has failed to publish the contact details of its Data Protection Officer on its official website or through any other medium that is readily accessible to the public. This omission deprives data subjects of a clear and accessible point of contact for data protection matters and is inconsistent with the transparency and accountability obligations imposed by the applicable data protection framework. Third, the policy lists the information collected by INEC but omits the sensitive ones like biometric data and the vast majority processed by the BVAs and iREV. This falls short of its transparency requirement.

The foregoing analysis demonstrates that, despite its central role in administering Nigeria's electoral process and its status as a controller of major importance, INEC's approach to transparency in personal data processing remains inadequate. Although the Commission subsequently published a privacy policy following litigation, the policy does not meaningfully address its principal data processing activities, particularly the collection and processing of voters' biometric and other sensitive personal data, nor does it comply fully with the statutory obligation to publish the contact details of its DPO. These deficiencies undermine the principles of transparency and accountability that underpin the NDPA and the GAID and diminish data subjects' ability to understand how their personal data are processed and to exercise their statutory rights effectively.

Footnotes

98 Suit. No. FHC/YNG/CS/148/26 between Inc. Trustees of Digital Rights Lawyers Initiative v Independent National Electoral Commission pending at the Federal High Court sitting in Yenogoa. See FIJ, 'FIJ Showed That INEC Broke Data Law, Digital Rights Lawyers Sue the Commission 10 Months Later' (FIJ, 2026) < http://fij.ng/article/fij-showed-that-inec-broke-data-law-digital-rights-lawyers-sue-the-commission-10-months-later/> accessed 12 September 2026.

99 Section 32(1) NDPA.

For an institution entrusted with the personal data of over 94 million Nigerians and charged with safeguarding the integrity of the democratic process, compliance with data protection obligations should not be reactive or litigation-driven but proactive, comprehensive and demonstrably aligned with both the letter and the spirit of Nigeria's data protection framework.

A further concern is that, even if INEC's publication of a privacy policy on its website were treated as an attempt to cure the identified transparency deficiency, its utility is necessarily limited by the digital accessibility of the affected data subjects.[100] INEC's National Register of Voters reportedly contains data relating to more than 94 million registered voters, yet not all of these individuals can reasonably be expected to have access to, or regularly consult, INEC's website. More importantly, the data subjects whose personal data are collected during voter registration are not necessarily the same persons who interact with INEC through its website. Voter registration is undertaken through physical registration centres and biometric enrolment processes, while the subsequent processing of fingerprints, facial images and other registration information occurs within INEC's electoral infrastructure. A privacy notice directed principally at website users therefore cannot, without more, satisfy the transparency obligation owed to the much larger population of persons whose personal data are processed for voter-registration purposes. Transparency under the NDPA is not merely an obligation to place information somewhere on the internet; it is an obligation to communicate relevant information to data subjects in a manner that enables them to understand how their personal data are being processed. Consequently, the publication of a privacy notice on INEC's website, while useful for persons who access the website, cannot by itself establish effective transparency towards the entire population of registered voters.

3.1.4 States' Independent Electoral Commissions' Compliance

To evaluate the data transparency posture of 36 SIECs, we developed a five-indicator assessment framework that captures both the existence and accessibility of privacy-related disclosures. The indicators examined: whether each SIEC maintains an official website; whether it has published a privacy policy; whether data protection information is available to users; and whether such information is accessible from prominent locations on the website, including the footer, main menu, or dedicated legal pages. These indicators are critical, as they reflect the foundational transparency obligations imposed on data controllers under the NDPA.[101]

The study's assessment was significantly hampered by a foundational challenge i.e the absence of a consistent and accessible digital presence across the SIECs. A considerable number of SIECs do not maintain independent websites,[102] opting instead to operate through state government portals that are not designed to host privacy-related disclosures. Others rely exclusively on social media platforms as their primary digital interface, while several Commissions maintain websites that are either inactive, inaccessible, or have not been updated for extended periods. This fragmented and often inadequate digital infrastructure not only complicates the assessment of data transparency compliance but also raises broader concerns about the SIEC's commitment to transparency and accountability in their data processing practices, particularly given their role as custodians of the personal data of millions of Nigerian citizens.

This concern becomes particularly significant in the electoral context, where the population of data subjects extends far beyond those who interact with the SIEC's digital platforms. A privacy notice published on a website may satisfy a degree of formal transparency, but its protective value is necessarily limited where large numbers of voters may have little or no access to the website or may not know that such a notice exists. The relevant question, therefore, is not merely whether the SIEC has published a privacy notice, but whether its transparency mechanisms are capable of reaching and informing data subjects irrespective of their access to its website. Effective data protection requires that voters be informed at, or in connection with, the points at which their personal data are collected and processed, using communication channels and formats reasonably accessible to them.[103] This is particularly important where the processing involves large-scale voter registration and biometric data, because the absence of meaningful notice may leave data subjects unaware of the nature and purposes of the processing, the entities with whom their data may be shared, applicable retention arrangements, and the rights available to them. Accordingly, the adequacy of the SIEC's transparency framework should be assessed not by the mere existence of a website privacy notice, but by whether the information provided is accessible, intelligible, contextually appropriate and capable of reaching the data subjects whose personal data are being processed. A website notice should therefore be regarded as one component of a broader transparency framework, rather than as a substitute for direct and inclusive mechanisms of voter information. Based on presently accessible information, very few SIECs publicly display privacy policies.

Footnotes

100 Mariavittoria Masotina and Anna Spagnolli, 'Transparency of Privacy Notices and Contextualisation: Effectively Conveying Information without Words' (2022) 41(10) Behaviour & Information Technology 2120.

101 For coding purposes, each indicator was recorded using a binary coding scheme of '1' (present) and '0' (absent). A website was coded as satisfying an indicator only where the relevant information could be located and accessed through the SIEC's publicly available website. The assessment did not treat the mere existence of a reference to data protection elsewhere on the internet as equivalent to publication on the SIEC's official website. Where a website was unavailable, inaccessible or technically non-functional during the assessment period, the compliance level was recorded as "low."

102 Unlike for INEC, there is no general provision in the Constitution or federal electoral legislation expressly requiring SIECs to maintain official websites. SIECs are principally established and regulated by state legislation, and the existence and nature of any website-related obligation must therefore be examined under the law establishing each particular Commission. This, however, does not mean that SIECs are free from obligations of transparency and accessibility. Where an SIEC processes voters' personal data, it is subject to the applicable obligations under the NDPA, including the requirement to provide data subjects with prescribed information concerning the processing of their personal data in an accessible manner. Thus, while the maintenance of a website may not, in itself, constitute a universal statutory requirement, the absence of an accessible online platform may raise legitimate questions about an SIEC's capacity to demonstrate compliance with its transparency, voter-information and data-protection obligations, particularly where substantial aspects of its electoral processes are conducted or communicated digitally.

103 Daniel Green, 'Strategic Indeterminacy and Online Privacy Policies: (Un)informed Consent and the General Data Protection Regulation' (2025) 38 International Journal for the Semiotics of Law 701.

a. Transparency Implication:

The assessment further reveals that although many SIEC websites collect personal data or provide contact channels, they do not appear to provide data subjects with the mandatory disclosures required under Section 27(1) of the NDPA, including the lawful basis for processing, retention periods, data subject rights, complaints procedures, and contact details for data protection matters. This gap is depicted in the table below.

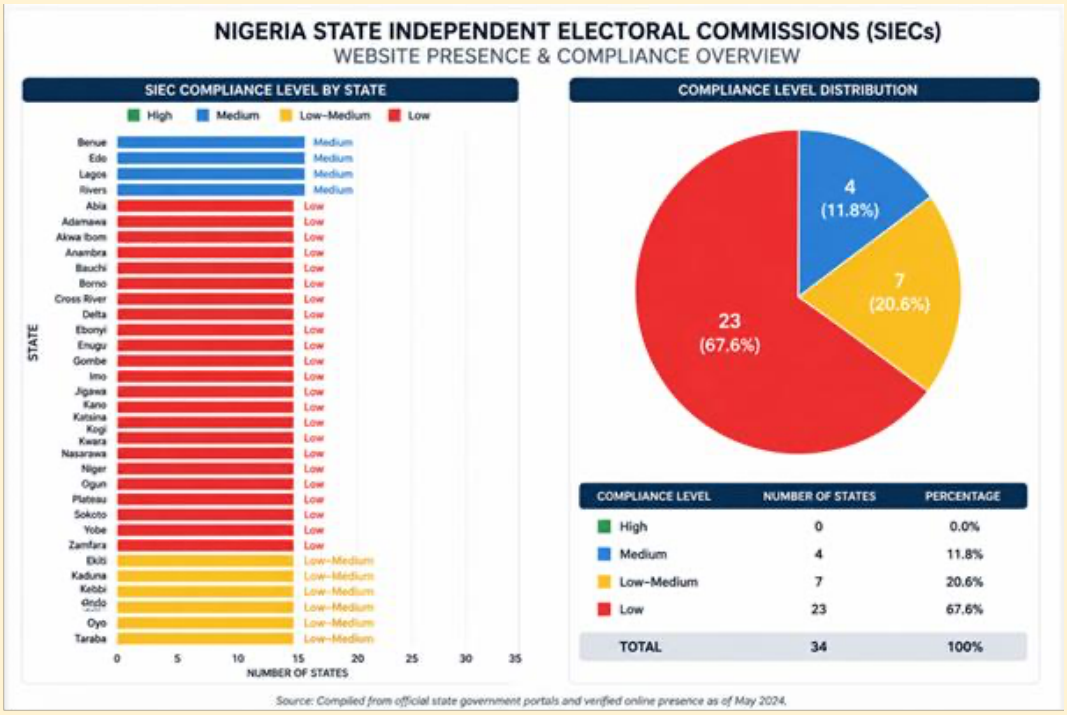
SIECs WEBSITE TRANSPARENCY TABLE (36 States)[104]

State	SIEC	Dedicated Website	Government Portal Only	Privacy Policy	Compliance Level
Abia	ABSIEC	No	No verified site	No	Low[105]
Adamawa	ADSIEC	No	No verified site	No	Low
Akwa Ibom	AKSIEC	No	No verified site	No	Low
Anambra	ANSIEC	No	No verified site	No	Low
Bauchi	BASIEC	No	No verified site	No	Low
Bayelsa	BYSIEC	No	No verified site	No	Low
Benue	BSIEC	Yes	No	No	Medium
Borno	BORSIEC	No	No verified site	No	Low
Cross River	CRSIEC	No	No verified site	No	Low
Delta	DSIEC	No	No verified site	No	Low
Ebonyi	EBSIEC	No	No verified site	No	Low
Edo	EDSIEC	Yes	Partial (also state portal)	No	Medium
Ekiti	EKSIEC	No	Yes	No	Low–Medium
Enugu	ENSIEC	No	No verified site	No	Low
Gombe	GOSIEC	No	No verified site	No	Low
Imo	IMSIEC	No	No verified site	No	Low
Jigawa	JISIEC	No	No verified site	No	Low
Kaduna	KDSIEC	No	Yes (state portal references only)	No	Low–Medium
Kano	KANSIEC	No	No verified site	No	Low
Katsina	KTSIEC	No	No verified site	No	Low
Kebbi	KBSIEC	No	Yes	No	Low–Medium
Kogi	KGSIEC	No	No verified site	No	Low
Kwara	KWSIEC	No	No verified site	No	Low
Lagos	LASIEC	Yes	Partial	No	Medium
Nasarawa	NASIEC	No	No verified site	No	Low
Niger	NGSIEC	No	No verified site	No	Low
Ogun	OGSIEC	No	No verified site	No	Low
Ondo	ODSIEC	No	Yes (state references only)	No	Low–Medium
Osun	OSSIEC	No	Yes (state references only)	No	Low–Medium
Oyo	OYSIEC	No	Yes (state references only)	No	Low–Medium
Plateau	PLSIEC	No	No verified site	No	Low
Rivers	RSIEC	Yes (limited access)	Partial	No	Medium
Sokoto	SOSIEC	No	No verified site	No	Low
Taraba	TSIEC	No	Yes (state portal only)	No	Low–Medium
Yobe	YOSIEC	No	No verified site	No	Low
Zamfara	ZASIEC	No	No verified site	No	Low

Footnotes

104 A structured web-based audit was conducted of the official websites of all 36 State Independent Electoral Commissions (SIECs) in Nigeria. The audit covered the period May 2026 to September 2026, with the final verification of website content undertaken on 30th day of September 2026. The 36 SIECs were selected as the population rather than as a sample because each State has a constitutionally established SIEC and the study seeks to assess the national state of data-protection transparency across the sub-national electoral management system. INEC itself confirms that Nigeria has 36 SIECs, each responsible for conducting local-government elections within its respective State. The audit employed a standardised, non-intrusive documentary review protocol. For each SIEC, the researchers first identified the Commission's official website through the Commission's own official channels, government portals or other authoritative sources. Each website (where available) was then assessed using the same predetermined checklist to ensure comparability across the 36 institutions. The audit examined, among other matters, (i) whether an operational official website was available; (ii) whether a privacy policy or privacy notice was published; (iii) whether the policy was readily accessible from the website; (iv) whether the identity and contact details of the controller were stated; (v) whether the lawful basis for processing was identified; (vi) whether the purposes and categories of personal data processed were disclosed; (vii) whether biometric or other sensitive personal data were addressed; (viii) whether information concerning data-subject rights and complaint mechanisms was provided; (ix) whether a DPO or privacy contact was identified; (x) whether information concerning third-party processors or data sharing was provided; and (xi) whether the privacy information was sufficiently clear, intelligible, transparent and easily accessible to satisfy the requirements of section 27(3) of the NDPA.

105 We deliberately adopted the classification of "low compliance" rather than "no compliance" because the absence of evidence or publicly available information should not, by itself, be treated as conclusive proof that no compliance measures exist. An electoral body may have adopted procedures, controls or other mechanisms that were not accessible to the researchers at the time of the assessment. Accordingly, the study does not equate the absence of publicly available evidence with absolute non-compliance. Rather, the applicable legal requirements were used as the principal and objective benchmark for assessing compliance. Where an institution provided no evidence of measures addressing a particular statutory requirement, its level of compliance was assessed as low, reflecting the limited evidence of conformity with the law, rather than conclusively declaring that no compliance measures whatsoever exist. This approach also recognises an important distinction between actual compliance and demonstrable compliance. For the purposes of an assessment, compliance must be capable of being demonstrated through identifiable policies, notices, procedures, institutional practices or other verifiable evidence. Where such evidence was unavailable, the study conservatively classified the institution as exhibiting low compliance rather than making the stronger finding of complete non-compliance.



The table and pie chart above show a pronounced digital transparency deficit across all the SIECs. Out of 36 states, only a small minority maintain any form of dedicated SIEC website (roughly about four states such as Lagos, Edo, Benue, and Rivers), while the majority either rely on fragmented state government portal pages or have no identifiable online presence at all. This indicates that online institutional visibility for SIECs is structurally weak and uneven, which immediately constrains the ability of these bodies to meet even baseline expectations of the NDPA 2023 transparency principle, which presupposes accessible public-facing information about data processing activities.

A second and more legally significant observation is the total absence of privacy governance artefacts across all categories. Even among the few SIECs with functional websites, none demonstrate a clearly identifiable privacy policy or NDPA-aligned privacy notice. Where SIECs are hosted on state government portals, the transparency gap is even more pronounced, as these pages typically function as informational directories rather than data governance interfaces. This creates a compliance asymmetry where institutions are operationally active in collecting and processing personal data (especially in electoral recruitment, accreditation, and staffing), yet they fail to operationalise the required disclosure mechanisms that would inform data subjects about lawful basis, retention periods, and rights under the NDPA.

Overall, the findings indicate a marked weakness in the publicly observable digital transparency of subnational electoral bodies, rather than conclusively establishing substantive non-compliance with the NDPA across all aspects of SIEC operations. Based on the single-pass review of publicly accessible SIEC websites, no SIEC was observed to combine a functioning dedicated digital presence with a readily accessible privacy or data-protection disclosure satisfying all of the indicators used in this study. The findings therefore suggest that, at least at the level of publicly visible digital infrastructure, NDPA transparency requirements have not yet been consistently integrated into SIEC website design and public-facing information practices.

This finding is particularly significant where an SIEC independently determines the purposes and means of processing substantial volumes of voter or electoral personal data and may therefore fall within the category of a data controller of major importance under section 44 of the NDPA. For such SIECs, the absence of accessible privacy and data-protection information may have greater implications for transparency, data-subject rights, accountability and regulatory oversight than in cases where an SIEC has limited independent digital infrastructure and relies substantially on state-government platforms or other shared systems. The study therefore distinguishes between the absence of publicly observable transparency mechanisms and a definitive finding of substantive NDPA non-compliance, while recognising that the former may provide an important indicator of institutional data-governance maturity and a basis for further regulatory inquiry. Accordingly, the results should be understood as identifying a digital transparency gap requiring further investigation, rather than as establishing that all 36 SIECs are substantively non-compliant with the NDPA. The findings nevertheless raise an important regulatory question: whether SIECs that independently process significant quantities of voter and electoral personal data have developed the governance, transparency and accountability architecture expected of controllers operating at that scale.

3.2 Filing of Annual Data Protection Compliance Audit Returns

3.2.1 Legal Framework

Under the NDPA and GAID, data controllers of major importance are required to file annual Compliance Audit Returns with the NDPC.[106] This filing demonstrates accountability and provides the regulator with visibility into compliance status across sectors.

3.2.2 The Findings

The NDPC's annual report indicated that Compliance Audit Returns filings increased from 1,864 filings in 2020–2021 to 4,691 filings in 2023–2024, indicating that more organisations are embracing data protection frameworks.[107] The Federal Government generated N12 billion from Nigeria's data protection sector in 2024, with compliance revenue rising sharply from N24.5 million in 2021 to N1.5 billion in 2024.[108]

However, there is no publicly available evidence that the NDPC has initiated enforcement action against a registered political party or electoral body for alleged non-compliance with data protection obligations. This may indicate either compliance with applicable filing and reporting requirements or that instances of non-compliance have not resulted in publicly disclosed enforcement action. The absence of enforcement should not, however, be treated as evidence of compliance, particularly given the scale and sensitivity of personal data processed within the electoral ecosystem.

Rather, it underscores the need for proactive, sector-specific regulatory scrutiny, including targeted compliance audits and inspections, verification of Compliance Audit Returns against actual processing practices, assessment of privacy notices, data-retention and security measures, and sector-specific guidance on biometric voter registration, voter-register management, political profiling and campaign communications. Comparable practice exists in the United Kingdom, where the Information Commissioner's Office has issued election-specific guidance and undertaken proactive engagement with political parties concerning electoral registers, political profiling, transparency and the processing of voters' personal data.[109] Accordingly, further regulatory scrutiny in Nigeria should move beyond reliance on self-reported compliance towards systematic monitoring, verification and, where necessary, enforcement capable of producing demonstrable accountability among electoral bodies and political actors.

3.2.3 Assessment of Compliance Level

	Subject to NDPA obligations?	Public evidence of CAR filing	Public evidence of non-filing	Assessment
Independent National Electoral Commission	Yes. INEC processes large volumes of voter and staff personal data.	None identified. No published CAR, annual privacy audit.[1]	None identified.	Compliance status unknown.
State Independent Electoral Commissions (SIECs)	Yes. SIECs process voter, electoral staff, and candidate data.	Ony Lagos SIEC filed CAR.[2]	None identified.	Compliance status unknown.

The table above reveals a significant gap in the public visibility of data protection compliance within Nigeria's electoral institutions. Although INEC and SIECs process substantial volumes of personal data and are therefore subject to data protection obligations, the study found no publicly available evidence of their Compliance Audit Returns or of regulatory enforcement actions against them. This absence of publicly accessible information does not, in itself, establish non-compliance, particularly where the applicable legal framework does not expressly require electoral institutions to publish their compliance filings or the outcome of regulatory engagements. Rather, it renders their actual level of compliance difficult to independently verify. The resulting uncertainty is significant in an electoral environment in which large-scale and sensitive personal data are processed, as it limits the ability of researchers, voters and other stakeholders to assess whether applicable data protection obligations are being effectively implemented and monitored. The issue, therefore, is not necessarily that INEC and SIECs have failed to comply, but that there is limited public visibility into the extent to which such compliance has been demonstrated, verified or subjected to regulatory oversight.

3.2.4 Data Breach Reporting and Incident Response Mechanisms

3.2.4.1 Legal Framework

Section 40 of the NDPA imposes specific obligations on data controllers in the event of a personal data breach. A data controller is required to notify the NDPC within 72 hours of becoming aware of a breach. Where the breach is likely to result in a high risk to the rights and freedoms of affected data subjects, the controller must also communicate the breach to those individuals without undue delay. In addition, data controllers are required to maintain records of all personal data breaches, including the nature and effects of the breach as well as the remedial measures taken to address it.

Footnotes

106 Referred to as 'Compliance Audit Returns' see section 6(d), 61(2)(g) GAID; Article 10, GAID.

107 Nigeria Data Protection Commission Annual Report 2024 found at https://ndpc.gov.ng/resources/> Accessed 24 June 2026.

108 See Govt earned N12bn from data protection in 2024 – NDPC found at < https://punchng.com/govt-earned-n12bn-from-data-protection-in-2024-ndpc/> Accessed 24 June 2026; < https://www.premiumtimesng.com/news/more-news/770409-nigeria-generated-n12bn-from-data-protection-in-2024-commission.html?> Accessed June 24, 2026.

109 Information Commissioner's Office, 'Guidance for the use of personal data in political campaigning' (ICO), particularly 'Use of the electoral register', 'Profiling in political campaigning' and 'Lawful, fair and transparent processing' <ICO, Guidance for the use of personal data in political campaigning> accessed 13 September 2026.

3.2.4.2. The Emeka Ike Breach: Reporting Compliance Analysis

The Emeka Ike data breach[110] serves as a critical case study for assessing the compliance of the INEC with the breach reporting obligations established under Section 40 of the NDPA.[111] This section examines the timeline of events surrounding the breach and evaluates INEC's conduct against the three core requirements of Section 40 on notification to the NDPC within 72 hours of becoming aware of a breach, communication with affected data subjects where the breach poses a high risk to their rights and freedoms, and comprehensive documentation of all breaches, including their effects and remedial actions taken.

The sequence of events reveals a troubling pattern of delayed response and inadequate transparency. In late May or early June 2026, leaked voter data belonging to Emeka Ike surfaced online, exposing sensitive personal information to public view. By June 1 to 2, 2026, INEC had acknowledged the breach and confirmed that it involved an insider, suggesting that the Commission had become aware of the incident and had conducted at least a preliminary investigation sufficient to identify the source of the leak. However, instead of demonstrating proactive compliance with its statutory obligations, INEC's response was reactive and limited in scope. On June 3, 2026, the Centre for Journalism Innovation and Development (CJID) issued a public statement calling on INEC to clarify whether it had notified the NDPC of the breach as required by law.[112] This intervention raises questions concerning whether INEC notified the NDPC of the incident as required by section 40(2) of the NDPA and whether the affected data subjects were appropriately informed where the statutory threshold for such notification was met. However, the absence of a public disclosure by INEC should not, in itself, be characterised as non-compliance, since the NDPA does not generally require a data controller to publicly disclose every personal data breach after notifying the Commission and affected data subjects. Rather, the absence of publicly available information makes it difficult to independently establish whether the statutory notification requirements were satisfied. The incident therefore illustrates a broader issue of the limited public visibility of data-protection compliance within the electoral sector, rather than necessarily demonstrating a failure by INEC to comply with its breach-notification obligations. The following day, on June 4, 2026, Emeka Ike spoke publicly about feeling "unsafe," underscoring the personal and tangible harm caused by the breach and highlighting the urgent need for effective communication with affected data subjects.[113]

3.2.4.3. Analysis of Compliance with Section 40 Obligations

When measured against the threefold obligations imposed by Section 40 of the NDPA 2023, INEC's conduct in the Emeka Ike case falls significantly short of the required standard.[114] The first immediately actionable obligation requires data controllers to notify the NDPC within 72 hours of becoming aware of a personal data breach. INEC became aware of the breach by at least June 1 to 2, 2026, when it publicly acknowledged the incident. Yet by June 3, 2026, the CJID was still calling on INEC to clarify its position regarding NDPC notification. This timing gap is deeply concerning for two reasons. First, if INEC had not notified the NDPC by June 3, it would have already exceeded the 72-hour statutory deadline, having been aware of the breach for at least one to two days. Second, even if INEC had notified the NDPC, its failure to state this publicly or include it in its initial acknowledgement reflects a lack of transparency that undermines public trust in the Commission's handling of sensitive personal data. The absence of any public confirmation from INEC that it had complied with this statutory obligation leaves open the possibility of systemic non-compliance.[115]

The second obligation under Section 40 requires data controllers to communicate the breach to affected data subjects without undue delay where the breach is likely to result in a high risk to their rights and freedoms. In this instance, the breach clearly posed a high risk to Emeka Ike's privacy and personal security, as evidenced by his own public statement on June 4, 2026, expressing that he felt "unsafe." The exposure of voter data, which may include sensitive personal information such as addresses, identification numbers, and other private details, carries inherent risks of identity theft, harassment, and other forms of harm. Despite this, there is no publicly available evidence that INEC directly notified Emeka Ike or any other affected individuals of the breach, its potential consequences, or the remedial measures available to them. Instead, Ike only became aware of the breach through public exposure and media reports, rather than through any formal notification from INEC. This represents a fundamental failure to protect data subjects' rights and disregards the very purpose of the notification requirement, which is to empower affected individuals to take protective measures in response to the breach.

The third obligation under Section 40 mandates that data controllers document all breaches, including their effects and the remedial actions taken.

Footnotes

110 See Olugbenga Ige, "INEC Probes Leak of Voter Data, Traces User Account," Punch Newspapers (2 June 2026) < https://punchng.com/inec-probes-leak-of-voter-data-traces-user-account/?utm_source>; Sodiq Omolaoye, "INEC, DSS Probe Alleged Voter Data Leak Involving Nollywood Actor," The Guardian Nigeria (3 June 2026) < https://guardian.ng/news/inec-dss-probe-alleged-voter-data-leak-involving-nollywood-actor/?utm_source> Accessed 26 July 2026.Solomon Odeniyi, "Voter Data Leak: Police Detain INEC Official, Quiz Wike's Aide," Punch Newspapers (4 June 2026) < https://punchng.com/voter-data-leak-police-detain-inec-official-quiz-wikes-aide/?utm_source> Accessed 26 July 2026. "Emeka Ike Sues Wike's Aide Over Alleged Exposure of INEC Data," The Guardian Nigeria (5 June 2026) < https://guardian.ng/politics/emeka-ike-sues-wikes-aide-over-alleged-exposure-of-inec-data/?utm_source> Accessed 26 July 2026. Adewale Edun, "Voter Data, Public Trust and Accountability: Emeka Ike–INEC Controversy," The Guardian Nigeria (8 June 2026) < https://guardian.ng/opinion/voter-data-public-trust-and-accountability-emeka-ike-inec-controversy/?utm_source > Accessed 26 July 2026. "Troubling Questions Dog INEC Data Leak," Punch Newspapers (18 June 2026) < https://punchng.com/troubling-questions-dog-inec-data-leak/?utm> Accessed 26 July 2026. Sami Tunji, "NDPC Probes INEC Over Emeka Ike's Data Leak," Punch Newspapers (20 June 2026) < https://punchng.com/ndpc-probes-inec-over-emeka-ikes-data-leak/?> Accessed 26 July 2026.

111 Nigerians outrage as INEC admits its personnel leaked confidential voter record of actor turned politician, Emeka Ike < https://www.pulse.ng/story/nigerians-outrage-as-inec-admits-its-personnel-leaked-confidential-voter-record-of-actor-turned-politician-emeka-ike-202606030923010068?> accessed 24 June 2026;

112 Centre for Journalism Innovation and Development, CJID Condemns Data Breach at INEC, Raises Serious Privacy and Data Protection Concerns' <https://thecjid.org/cjid-condemns-data-breach-at-inec-raises-serious-privacy-and-data-protection-concerns/?> Accessed 25 June 2026

113 Hannah Johnson, 'I felt unsafe for the first time, Emeka Ike cries out over INEC data leak' < https://punchng.com/i-felt-unsafe-for-the-first-time-emeka-ike-cries-out-over-inec-data-leak/?utm_source> 24 June 2026.

114 Mfon Daniel, 'Wike's Aide Has No Right To Expose My Privacy' — Emeka Ike Vows Action Over INEC Data Leak' < https://politicsnigeria.com/2026/06/02/wike-has-no-right-to-expose-my-privacy-emeka-ike-vows-action-over-inec-data-leak/?utm_source> Accessed 24 June 2026.

115 Since the NDPA does not impose a general obligation on a controller to publicly announce every instance of compliance. Nevertheless, this does not render public disclosure irrelevant to INEC's data-protection responsibilities. The NDPA imposes duties of care and accountability on data controllers and requires controllers to demonstrate compliance with its data-protection principles. In the case of INEC, these obligations must also be understood in the context of its statutory character as the institution responsible for administering Nigeria's elections and its corresponding obligations of transparency and accountability in the discharge of its public functions. Accordingly, where INEC undertakes significant measures to protect voters' personal data, particularly following a data-protection incident, making appropriate information about such measures publicly accessible would promote demonstrable accountability and enable voters and other stakeholders to assess how their personal data is being protected. This is particularly important in the electoral context, where public confidence is indispensable to the legitimacy of the electoral process. Thus, the concern is not that the absence of a public confirmation necessarily constitutes a breach of the NDPA, but that, even where the underlying legal obligations have been fulfilled, the absence of meaningful public information about INEC's data-protection measures may diminish the visibility of compliance, impede independent scrutiny and undermine public trust in the institution's stewardship of voters' personal data.

The purpose of this requirement is to ensure accountability, facilitate learning from incidents, and provide a record that can be reviewed by the NDPC and other oversight bodies. Even though there is no express obligation to publicly disclose such documentation, international practices favour these accountability and transparency metrics.[116]

INEC has not publicly disclosed any such documentation in relation to the Emeka Ike breach, nor has it provided a comprehensive account of the remedial measures it has implemented to prevent future occurrences. The absence of such documentation is particularly concerning given that INEC confirmed insider involvement, which suggests a systemic vulnerability that requires urgent attention and remediation. Without a transparent record of the breach's effects and the actions taken in response, stakeholders including the public, civil society organisations, and the NDPC are left without the information necessary to assess INEC's data protection practices and hold the Commission accountable.

3.2.4.4. Implications and Broader Conclusions

The Emeka Ike breach and INEC's response to it reveal a troubling pattern of non-compliance with the NDPA that extends beyond this single incident. INEC, as the primary custodian of Nigeria's voter register, processes vast amounts of sensitive personal data on millions of citizens, placing it squarely within the category of data controllers of major importance subject to the highest standards of data protection compliance. Yet its conduct in this case demonstrates a reactive rather than proactive approach to breach management, characterised by delayed acknowledgement, inadequate notification, and a lack of transparency. The Commission's failure to demonstrate compliance with Section 40 suggests either a disregard for the statutory obligations imposed by the NDPA 2023 or a systemic incapacity to meet those obligations effectively.

Furthermore, the absence of any public evidence that the NDPC has taken enforcement action or issued a public reprimand in response to this incident raises broader questions about the effectiveness of Nigeria's data protection enforcement ecosystem. If a major public institution can experience a significant data breach involving insider involvement and fail to demonstrate compliance with the core reporting obligations without consequence, the deterrent effect of the NDPA 2023 is seriously undermined. This case also highlights the critical need for the NDPC to strengthen its public communication and enforcement mechanisms to ensure that data controllers, particularly in the public sector, understand and comply with their obligations.

Footnotes

116 International practice demonstrates that the existence of an internal data-breach register does not necessarily preclude public disclosure of information concerning recorded breaches. In New South Wales, Australia, for example, the Department of Customer Service publishes a Data Breach Public Notification Register where it is unable or it is not reasonably practicable to notify affected individuals directly; the public register may disclose the date and description of the breach, how it occurred, the type of breach and information affected, and measures taken to mitigate the harm. See NSW Department of Customer Service, 'DCS Data Breach Public Notification Register' (NSW Government, 4 July 2024) https://www.nsw.gov.au/departments-and-agencies/customer-service/dcs-data-breach-register A similar distinction is maintained by the State Insurance Regulatory Authority (SIRA), which expressly maintains an internal breach register but publishes an external register for eligible breaches where individual notification is impracticable, while excluding personal information and information that could prejudice its functions. The same model operates across other NSW public authorities, including the National Education Standards Authority, which is required to maintain a public notification register containing specified information about eligible breaches, subject to exclusions for personal information and material that could prejudice its functions. State Insurance Regulatory Authority (NSW), 'SIRA Data Breach Response Policy' (NSW Government) https://www.sira.nsw.gov.au/privacy/sira-privacy-docs/sira-data-breach-response-policy accessed 13 September 2026. The United Kingdom provides another model of institutional transparency: the Cabinet Office has publicly disclosed the number of ICO-recordable breaches recorded by the department through its annual reports, while the Information Commissioner's Office publishes aggregate data on data-security incidents reported to it by organisations. The ICO's 2024–25 Annual Report, for instance, publicly reported 12,412 personal-data breach reports received during the year. See UK Parliament, 'Data breaches: Cabinet Office' (Written Question UIN 70973, 13 July 2020) https://questions-statements.parliament.uk/written-questions/detail/2020-07-08/70973 accessed 13 September 2026.

CHAPTER 4
POLICY RECOMMENDATIONS



The assessment conducted in the previous chapters reveals a pattern of systemic, structural non-compliance by Nigeria's electoral bodies with the transparency, accountability, and data subject rights obligations imposed by the NDPA and GAID. The absence of a privacy policy on INEC's website until compelled by litigation, the complete lack of NDPA-aligned privacy governance artefacts across the 36 SIECs, the unresolved status of Compliance Audit Return filings, and the delayed, opaque handling of the Emeka Ike breach are not isolated failures[117] but symptoms of a governance environment in which data protection compliance is reactive, under-resourced, and largely unenforced. The recommendations that follow are designed to convert this reactive posture into a proactive, institutionalised, and enforceable framework of privacy governance across the electoral ecosystem, addressing legislative gaps, regulatory oversight, institutional capacity, technological safeguards, transparency practices, data subject rights enforcement, personnel training, and public awareness.

PILLAR I — LEGISLATIVE AND REGULATORY REFORM

4.1 Legislative and Regulatory Reforms

The current legal architecture governing electoral data protection is fragmented across the NDPA 2023, the Electoral Act 2026, and the GAID, none of which speaks directly and comprehensively to the peculiarities of electoral data processing. The following reforms are recommended:

4.1.1 Issue a sector-specific Electoral Data Protection Code of Practice, issued by the NDPC pursuant to its power to issue guidelines and codes of practice under the NDPA, to translate the general principles of the Act into concrete, electoral-specific obligations for INEC and SIECs, covering voter registration, biometric capture, BVAS and IReV operations, and third-party vendor management.[118]

4.1.2 Amend the Electoral Act to expressly codify the lawful basis for the mandatory collection of biometric data during voter registration as processing necessary for compliance with a legal obligation and for the performance of a task carried out in the public interest, rather than leaving this foundational question to inference from Section 30 of the NDPA on sensitive. Codification would remove the ambiguity identified in this study regarding whether consent obtained under conditions where refusal forfeits the right to vote can be considered "freely given."[119]

4.1.3 Introduce a statutory pre-registration compliance requirement obliging INEC and each SIEC to publish a comprehensive, NDPA-compliant privacy notice not later than a fixed number of days (for example, thirty days) before the commencement of any continuous voter registration or fresh registration exercise, with failure to publish the notice within the prescribed period constituting a regulatory compliance violation subject to appropriate sanctions under the NDPA."[120]

4.1.4 Insert express, electoral-specific administrative sanctions into the Electoral Act for breaches of data protection obligations by electoral bodies, operating in tandem with (not as a substitute for) the NDPC's enforcement powers, to ensure that electoral non-compliance carries consequences even where NDPC enforcement capacity is stretched.[121]

4.2 Strengthening NDPC Oversight of Electoral Bodies

This study found no publicly available evidence that the NDPC has conducted a compliance audit of, or taken enforcement action against, INEC or any SIEC, despite these bodies collectively controlling the most extensive biometric database in the country. Oversight has, to date, been triggered by litigation and media exposure rather than by proactive regulatory supervision. The following measures are recommended:

4.2.1 The NDPC should establish a dedicated Electoral and Political Data Protection Desk responsible for continuous, year-round supervision of INEC, all 36 SIECs and registered political parties, rather than limiting regulatory engagement to the immediate pre-election period. The Desk should maintain an electoral-data compliance register, coordinate periodic risk assessments and audits, monitor voter-registration and biometric-data processing, supervise third-party technology vendors, receive and escalate electoral-data breach reports, and coordinate with electoral bodies on remedial measures. Its mandate should extend across the complete electoral-data lifecycle, from voter registration and biometric capture through accreditation, results transmission, retention and eventual deletion or archival disposal. This recommendation is supported by the NDPA's allocation of regulatory and supervisory functions to the NDPC, including its responsibilities to regulate the deployment of technological and organisational measures for personal-data protection and to ensure compliance with data-protection obligations and best practice. The recommendation is particularly justified by the scale and sensitivity of electoral databases: the NDPC reported in April 2026 that INEC holds the personal data of approximately 94 million Nigerians and, in response, inaugurated a joint NDPC–INEC working group to integrate data protection and privacy into the electoral system.[122]

4.2.2 The NDPC should institute a structured electoral-sector audit programme requiring INEC and every SIEC to undergo scheduled data-protection compliance audits at least annually and, where practicable, a heightened

Footnotes

117 For example, rather than INEC itself reporting the data breach to the NDPC, it was the affected data subject, Emeka Ike, who initiated the complaint by petitioning the NDPC concerning the alleged disclosure of his personal data. Sami Tunji, 'NDPC probes INEC over Emeka Ike's data leak' Punch (20 June 2026) https://punchng.com/ndpc-probes-inec-over-emeka-ikes-data-leak/

118 Sections 5(a), 5(i), 5(n), 6(c), together with section 61(2)(b) and (i) NDPA. Comparative lessons can be taken from the Council of Europe, 'Guidelines on the Protection of Individuals with regard to the Processing of Personal Data for Voter Registration and Authentication' (18 September 2024)

119 Nigeria Data Protection Act 2023, ss 25, 30, 65. See also European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Data Protection Law (2018).

120 See UK Electoral Commission, 'Data protection guidance for Electoral Registration Officers and Returning Officers: Privacy notices – the right to be informed' (updated 22 February 2023); Council of Europe, 'Guidelines on the Protection of Individuals with regard to the Processing of Personal Data for Voter Registration and Authentication' (18 September 2024) and Olumide Babalola, 'Data Protection in E-Voting Systems: The 2024 Nigerian Bar Association's Elections in Retrospect' (2025) 13(1) ABUAD Law Journal.

121 See Nigeria Data Protection Commission, 'FAQs' (confirming the Commission's enforcement and remedial powers under s 48 NDPA); African Union, AU Data Policy Framework (2022); Council of Europe, 'New guidelines to protect voters' personal data' (18 September 2024).

122 Ahmad Nur Hidayat, Nina Karlina, Ramadhan Pancasilawan and R Widya Setiabudi Sumadinata, 'How electoral management bodies govern digital electoral systems: capacity, authority, and accountability' (2026) 8 Frontiers in Political Science 1877569; Nigeria Data Protection Act 2023, ss 5(a), 5(i), 6(c), 61(2)(b), (i); Nigeria Data Protection Commission, 'Securing 94 million Identities: NDPC and INEC Form Strategic Pact to Safeguard Voter Privacy' (15 April 2026).

compliance review before each general election. The audits should cover governance arrangements, data-processing activities, biometric-data protection, technical and organisational security measures, data-retention practices, third-party processors and technology vendors, data-subject rights, breach preparedness, and transparency obligations. Rather than publishing complete audit reports where doing so could expose security-sensitive or confidential information, the NDPC should publish summarised and appropriately redacted audit outcomes, identifying the institution audited, principal areas examined, material deficiencies, remedial measures required and the status of remediation. Such a framework would convert the present uncertainty concerning the compliance status of electoral bodies into an observable regulatory accountability mechanism. It is also consistent with the NDPC's treatment of Compliance Audit Returns as an accountability mechanism: its 2023 Annual Report described CARs as a 'potent tool of accountability' and recorded 1,674 audit filings, while its April 2026 IMPACT initiative expressly characterised CARs as a means of demonstrating accountability and managing privacy risks. [123]

4.2.3 The NDPC should formalise the joint working arrangement inaugurated with INEC in April 2026 through a binding memorandum of understanding or equivalent regulatory instrument containing clearly defined deliverables, implementation timelines, institutional responsibilities, reporting requirements and measurable compliance indicators. The arrangement should incorporate sustained privacy-management, information-security and staff-capacity-building measures, including appropriate alignment with internationally recognised standards such as ISO/IEC 27701 for privacy information management and ISO/IEC 27001 for information security management. An equivalent institutional framework should be developed between the NDPC and the Forum of State Independent Electoral Commissions of Nigeria (FOSIECON) to facilitate coordinated supervision and capacity-building across the SIECs. This would transform the existing NDPC–INEC collaboration from an important but largely cooperative initiative into a structured mechanism of continuing regulatory accountability. The proposal is also consistent with the NDPC's own April 2026 recognition that electoral data protection requires engagement not only with INEC but also with political parties, civil society organisations, third-party service providers and vendors.[124]

4.2.4 The NDPC should apply its existing enforcement powers consistently to electoral bodies found to have violated the NDPA or applicable subsidiary legislation, including the issuance of remedial orders, compliance directions, compensation orders and applicable administrative penalties. Where legally permissible and subject to the protection of confidential, security-sensitive or personal information, the Commission should publish sufficiently detailed enforcement outcomes to communicate the nature of the violation, the institution concerned, the remedial measures imposed and the status of compliance. Such publication would enhance deterrence, institutional learning and public confidence in the enforcement of data-protection obligations within the electoral sector. The recommendation assumes particular significance in light of the alleged disclosure of Emeka Ike's voter-registration information. The NDPC commenced an investigation into the incident in June 2026 and engaged both INEC and the affected individual. Accordingly, the issue is not the absence of regulatory intervention, but the need for the eventual outcome of such investigations, where legally appropriate, to produce visible and accountable enforcement or remedial action.[125]

4.2.5 The National Assembly and the relevant state legislative authorities should consider introducing an appropriate legislative or budgetary mechanism requiring INEC and SIECs to demonstrate compliance with their mandatory data-protection audit obligations as part of election-related appropriation and accountability processes. Such compliance should include timely filing of the required Compliance Audit Returns and, where appropriate, submission of evidence of remediation of material deficiencies identified through the audit process. Rather than making the publication of complete CARs an automatic condition of funding, the NDPC should publish a compliance status or appropriately redacted summary indicating whether the relevant electoral body has fulfilled its audit obligations and whether material deficiencies remain outstanding. The objective should not be to confer upon the executive a discretionary power to withhold constitutionally or statutorily protected electoral funding, but to integrate data-protection compliance into existing mechanisms of legislative appropriation, audit and institutional accountability. This would recognise that the protection of voter data is not merely a technical compliance matter but an integral component of the integrity of the electoral process.[126]

Footnotes

123 Nigeria Data Protection Act 2023, ss 24(2), 61(2)(g); Nigeria Data Protection Commission, Nigeria Data Protection Annual Report 2023 (2024) 15; Nigeria Data Protection Commission, 'NDPC Hosts 3rd IMPACT Initiative: Positions Compliance Audit Returns as Key to Corporate Risk Management' (10 April 2026); Nigeria Data Protection Commission, Nigeria Data Protection Act 2023, General Application and Implementation Directive (GAID) 2025, art 10.

124 Nigeria Data Protection Commission, 'Securing 94 Million Identities: NDPC and INEC Form Strategic Pact to Safeguard Voter Privacy' (15 April 2026); Nigeria Data Protection Commission, 'Setting the Gold Standard: NDPC Pursues ISO 27001 and 27701 to Fortify National Data Trust' (20 April 2026); Nigeria Data Protection Act 2023, ss 5, 6, 61; Habiba Musa, 'Data Protection Issues in the Management of the Bimodal Voters Accreditation System (BVAS) in Nigeria' (2023) 10(2) Nnamdi Azikiwe University Journal of Commercial and Property Law 65; Hidayat et al (n above).

125 Nigeria Data Protection Act 2023, ss 46–48; Nigeria Data Protection Commission, Nigeria Data Protection Annual Report 2023 (2024) 15; Sami Tunji, 'NDPC probes INEC over Emeka Ike's data leak' Punch (20 June 2026); Hidayat et al (n above).

126 Nigeria Data Protection Act 2023, ss 24(3), 61(2)(g), (i); Nigeria Data Protection Commission, General Application and Implementation Directive (GAID) 2025, art 10; Nigeria Data Protection Commission, Nigeria Data Protection Annual Report 2023 (2024) 15; Nigeria Data Protection Commission, 'NDPC Hosts 3rd IMPACT Initiative: Positions Compliance Audit Returns as Key to Corporate Risk Management' (10 April 2026)

PILLAR II — INSTITUTIONAL AND OPERATIONAL COMPLIANCE

4.3 Institutionalisation of Privacy Governance Frameworks

Beyond legislative and regulatory reform, sustainable compliance requires that privacy governance be embedded within the internal structures of INEC and the SIECs, rather than treated as an external, litigation-driven obligation. The following institutional measures are recommended:

4.3.1 Mandatory appointment of a substantive Data Protection Officer (DPO) by INEC and each SIEC, with the DPO's contact details published prominently on the institution's website and, where no dedicated website exists, on the relevant state government portal, in compliance with Section 32 of the NDPA and Article 11(2) of the GAID.[127]

4.3.2 INEC should establish an internal Data Protection Governance Unit, with a parallel and appropriately scaled function within each SIEC, supported by a distinct budgetary allocation, clear reporting lines to the institution's leadership and adequate personnel and technical resources. The Unit should coordinate privacy compliance across the electoral data lifecycle, maintain comprehensive records of processing activities, coordinate Data Protection Impact Assessments, monitor processors and third-party vendors, support the DPO in regulatory reporting, and maintain evidence of compliance and remediation. Such institutionalisation would give practical effect to the accountability obligation in section 24(3) of the NDPA, which requires controllers and processors to demonstrate accountability, while ensuring that data protection is embedded within electoral administration rather than treated as an ancillary function.[128]

4.3.3 INEC should revise its privacy policy, while each SIEC should develop and publish a comprehensive privacy policy appropriate to its processing activities. These policies should address the principal stages of the electoral data lifecycle, including voter registration, collection and processing of biometric information, voter verification and accreditation, BVAS-related processing, results transmission and IReV-related data flows, data sharing with authorised public authorities, processing by third-party technology providers, retention periods, security measures, data-subject rights, breach management and applicable lawful bases. Privacy information should be presented in clear, concise, transparent and easily accessible language and should be made available at the point at which voters' personal data are collected.[129] The recommendation is supported by section 27 of the NDPA, which requires controllers collecting personal data directly from data subjects to provide specified information concerning the controller, purposes and lawful basis of processing, recipients, retention and data-subject rights, while requiring the relevant privacy policy to be clear, concise, transparent, intelligible and easily accessible. The need for an electoral-specific privacy framework is particularly compelling given the scale and sensitivity of the data processed by INEC, including biometric information.

4.3.4 INEC and SIECs should formalise written Data Processing Agreements with every third-party technology vendor processing personal data on their behalf and should incorporate data-protection requirements into procurement and service contracts. These agreements should contain, at a minimum, provisions governing the purpose and scope of processing, lawful basis, confidentiality, technical and organisational security measures, audit and inspection rights, restrictions on sub-processors, data-retention and deletion obligations, cross-border transfers, incident-management procedures and clearly defined breach-notification timelines aligned with section 40 of the NDPA. Contracts should also require vendors to provide information and documentation necessary for the electoral body to demonstrate compliance, and should make material non-compliance a ground for contractual remediation, suspension or termination.[130] This recommendation gives practical effect to section 29 of the NDPA, which regulates processing by data processors and requires the controller and processor to enter into a written agreement governing the processing relationship. Article 35 of the GAID further specifies the matters to be addressed in a Data Processing Agreement, including the purpose and scope of processing, lawful basis, responsibilities of the parties, technical and organisational measures, DPIA outcomes, confidentiality and restrictions. Given the extensive involvement of technology providers in voter registration, biometric processing and electoral information systems, contractual governance should form an integral part of electoral data protection compliance.

4.3.5 Formalisation of data processing agreements with all third-party technology vendors involved in the electoral data ecosystem, incorporating mandatory security audit rights, restrictions on the engagement of sub-processors without prior authorisation, and contractual breach-notification timelines aligned with Section 40 of the NDPA, consistent with the obligations already imposed on data controllers under Section 29.

Footnotes

127 Nigeria Data Protection Act 2023, s 32; Nigeria Data Protection Commission, General Application and Implementation Directive (GAID) 2025, arts 11–14; Thando Sibanda, 'Facilitating Privacy Compliance in Nigeria: Key Issues in the GAID Draft 2024' (CIPIT).

128 Nigeria Data Protection Act 2023, s 24(3); Nigeria Data Protection Commission, General Application and Implementation Directive (GAID) 2025, arts 7, 12–13; Jinkai Abinkallo Kato, 'Data Subject Rights in Nigeria: Bridging the Gap Between Policy and Practice' (2026) 2nd edn, NDPC International Journal of Data Privacy and Protection 86, 87.

129 INEC's current general privacy policy expressly states that it concerns people who visit or interact with the INEC website and digital services, and identifies information such as names, emails, telephone numbers, postal addresses, enquiries, complaints and recruitment documents. It is however noted that upon the conclusion of this study and the institution of an action against INEC (supra), they now have a separate Personal Biometric Registration Application privacy policy, effective July 2026. That policy expressly addresses biometric enrolment, transmission to INEC backend systems, disclosure to authorised service providers, retention on devices and DPO contact information. See https://cvr.inecnigeria.org/legal?utm_source> accessed 13 September 2026.

130 Nigeria Data Protection Act 2023, ss 29, 40; GAID 2025, art 35.

4.4. Mandatory DPIAs for Electoral Technologies

The processing of biometric and demographic data belonging to over 94 million registered voters through systems such as the Bimodal Voter Accreditation System (BVAS), the INEC Result Viewing Portal (IReV), and the Continuous Voter Registration (CVR) database unquestionably meets the high-risk threshold that triggers the Data Protection Impact Assessment (DPIA) requirement under Section 28 of the NDPA. The following measures are recommended:

4.4.1 Make the conduct of a DPIA a mandatory precondition, enforceable by the NDPC, before the deployment of any new electoral technology or any material upgrade to an existing system such as BVAS or IReV, with the assessment addressing necessity and proportionality, security risks including unauthorised access and misuse of biometric data, and the technical and organisational safeguards to be implemented.[131]

4.4.2 INEC should publish a redacted summary of each DPIA undertaken in relation to significant electoral technologies, including BVAS, IReV and any successor systems. The summary should disclose the nature and purpose of the processing, categories of personal data involved, principal risks identified, the necessity and proportionality assessment, broad categories of technical and organisational safeguards, and any material residual risks or remedial measures. Information capable of facilitating cyberattacks, compromising system security, revealing authentication mechanisms or otherwise creating material security vulnerabilities should be withheld. Such graduated disclosure would allow voters, civil-society organisations and other stakeholders to evaluate whether electoral technologies have been subjected to meaningful privacy-risk assessment without requiring the publication of security-sensitive technical information.[132]

4.4.3 The NDPC should extend to the SIECs the privacy-management training, assessment and capacity-building initiatives being developed in collaboration with INEC, including, where appropriate, training and assessment based on ISO/IEC 27701 for Privacy Information Management Systems. This should be accompanied by proportionate implementation guidance enabling SIECs to identify, assess and mitigate privacy risks associated with voter registration, biometric processing, voter authentication and electoral-result technologies. The extension is justified by the fact that the privacy risks associated with biometric and demographic electoral data do not disappear at the subnational level but arise across the electoral system wherever personal data are collected and processed at scale.[133]

4.4.4 DPIAs relating to electoral technologies should be treated as living risk-management instruments rather than one-off compliance documents. INEC and SIECs should be required to review and, where necessary, update each relevant DPIA before every major electoral cycle and whenever there is a material change in the technology, processing purpose, volume or categories of personal data, vendor or processor arrangements, system architecture, security environment or identified risk profile. The reassessment should determine whether previously identified risks and safeguards remain adequate and whether additional technical, organisational or legal safeguards are required. This approach would ensure that DPIAs remain responsive to changes in electoral technology and the evolving threat environment rather than becoming static documents prepared merely to satisfy an initial regulatory requirement.[134]

4.5 Standardisation of Privacy Notices and Consent Practices

The stark disparity between INEC's belatedly published but incomplete privacy policy and the near-total absence of privacy notices across the SIECs, documented in the transparency assessment in Chapter Four, demonstrates the need for a standardised, minimum-content approach across all electoral bodies. The following measures are recommended:

4.5.1 The NDPC should issue a standard-form privacy notice template specifically tailored to electoral bodies, prescribing minimum information to be provided to voters in accordance with section 27(1) of the NDPA and article 27 of the GAID. The template should require electoral bodies to identify the applicable lawful basis for each principal processing activity; specify the categories of personal and sensitive personal data collected; state the purposes and means of processing; identify authorised third parties and vendors and the purposes for which they may access voter data; specify applicable retention periods; explain the rights available to data subjects and the procedure for exercising those rights; and provide contact details for the relevant Data Protection Officer and the NDPC. The template should be sufficiently standardised to promote consistency across INEC and the SIECs while permitting institution-specific information to be incorporated.[135]

4.5.2 The NDPC should, either through sector-specific guidance or the proposed Electoral Data Protection Code, expressly clarify the appropriate lawful basis for mandatory biometric processing undertaken for voter registration and authentication.

Footnotes

131 Nigeria Data Protection Act 2023, s 28(1), (4).

132 Nigeria Data Protection Act 2023, s 28(4); Nigeria Data Protection Commission, General Application and Implementation Directive (GAID) 2025, art 23 and art 28(11); Alexander B Makulilo, 'Rebooting democracy? Political data mining and biometric voter registration in Africa' (2017) 26(2) Information & Communications Technology Law 198.

133 Nigeria Data Protection Commission, 'Securing 94 Million Identities: NDPC and INEC Form Strategic Pact to Safeguard Voter Privacy' (15 April 2026); Nigeria Data Protection Commission, 'Setting the Gold Standard: NDPC Pursues ISO 27001 and 27701 to Fortify National Data Trust' (20 April 2026); Nigeria Data Protection Commission, Nigeria Data Protection Commission Annual Report 2025 (2026);

134 Nigeria Data Protection Act 2023, s 28; Nigeria Data Protection Commission, General Application and Implementation Directive (GAID) 2025, art 28 and sch 4;

135 Nigeri Every SIEC should be required to publish a privacy notice conforming to the NDPC's standard electoral privacy-notice template. Where an SIEC maintains a functional website, the notice should be prominently and permanently accessible from that website; where it does not maintain a dedicated website, the relevant state government portal should provide a clearly signposted and dedicated data-protection page through which the SIEC's privacy notice can be accessed. The absence of a dedicated website should not operate as a justification for the absence of publicly accessible privacy information. The NDPC should incorporate verification of the accessibility, completeness and currency of SIEC privacy notices into its periodic compliance audits.a Data Protection Act 2023, s 27(1); GAID 2025, art 27(1), (3).

The framework should distinguish compulsory electoral processing, which should rest on a clearly identifiable statutory legal obligation and/or public-interest mandate supported by law and appropriate safeguards, from genuinely voluntary processing for which consent may be appropriate. This clarification would address the coercion concern identified in this study by preventing electoral bodies from presenting mandatory biometric capture as consent-based processing where refusal would prevent or materially impede access to the electoral process. The clarification should, however, make equally clear that reliance on a legal obligation or public-interest basis does not displace the electoral body's independent transparency and accountability obligations under section 24(1)(a) and section 27 of the NDPA and article 27 of the GAID.

4.5.3 Every SIEC should be required to publish a privacy notice conforming to the NDPC's standard electoral privacy-notice template. Where an SIEC maintains a functional website, the notice should be prominently and permanently accessible from that website; where it does not maintain a dedicated website, the relevant state government portal should provide a clearly signposted and dedicated data-protection page through which the SIEC's privacy notice can be accessed. The absence of a dedicated website should not operate as a justification for the absence of publicly accessible privacy information. The NDPC should incorporate verification of the accessibility, completeness and currency of SIEC privacy notices into its periodic compliance audits.[136]

PILLAR III — ENFORCEMENT, ACCOUNTABILITY AND PUBLIC REDRESS

4.6 Improvement of Data Subject Rights Response Mechanisms

The Emeka Ike breach demonstrated that, even where a data subject suffers tangible harm from a compromise of their voter data, Nigeria's electoral bodies presently lack a demonstrable, transparent mechanism for responding to affected individuals or facilitating the exercise of their statutory rights. The following measures are recommended:

4.6.1 INEC and each SIEC should establish and clearly publicise dedicated channels through which voters may exercise their data-subject rights and submit complaints. Such channels may include a dedicated email address, web portal, telephone line, or designated physical point of contact, depending on the institution's technological capacity. The channels should facilitate, at a minimum, requests for access and rectification and complaints concerning the processing of voter data, while providing appropriate mechanisms for other applicable data-subject rights.

Each electoral body should publish clear procedures for submitting requests, identify its Data Protection Officer or designated privacy contact, and establish reasonable internal turnaround targets for acknowledging and resolving requests. This would give practical effect to the rights guaranteed under sections 34–38 of the NDPA and the accessibility requirements applicable to the exercise of data-subject rights under the GAID.[137]

4.6.2 INEC and each SIEC should develop and maintain standard operating procedures (SOPs) governing the receipt, verification, recording, escalation and resolution of data-subject requests and complaints. The SOPs should assign responsibility to relevant officers, establish internal response and escalation timelines, provide mechanisms for documenting decisions and reasons for refusal, and prescribe circumstances in which matters must be referred to the DPO or senior data-governance personnel. Internal timelines should be sufficiently short to enable the electoral body to comply with its statutory and regulatory obligations without avoidable delay. The SOPs should also establish a clear interface between ordinary data-subject requests and incident-response procedures where a request reveals a suspected personal-data breach.[138]

4.6.3 INEC and each SIEC should institutionalise a formal personal-data breach-response protocol that operationalises the obligations imposed by section 40 of the NDPA and article 34 of the GAID. The protocol should provide for the immediate identification and containment of suspected breaches; prompt assessment of the nature, scope and likely consequences of the incident; notification to the NDPC within 72 hours where the breach is likely to result in a risk to the rights and freedoms of individuals; communication with affected data subjects without undue delay where the breach is likely to result in a high risk to their rights and freedoms; and contemporaneous documentation of the breach, its effects, notifications, containment measures and remedial actions. The protocol should also designate responsible officers, escalation pathways and decision-making authority. Standardised notification templates should be prepared in advance so that legally required information can be communicated accurately and promptly during an incident. The protocol should be supported by periodic simulation exercises and post-incident reviews, particularly because electoral databases may contain large volumes of identifying and biometric information and unauthorised disclosure may have consequences extending beyond ordinary information-security risks. The objective should therefore be to ensure that breach response is an institutionalised governance process rather than an improvised reaction to an incident.[139]

Footnotes

136 Nigeria Data Protection Act 2023, ss 24(1)(a), 27(1), (3); GAID 2025, art 27

137 Nigeria Data Protection Act 2023, ss 27, 34–38; General Application and Implementation Directive 2025 (GAID 2025), arts 27, 36 and 45; Faith Amarachi Okpara and Chinonso Queenesther Emeka, 'Data Subject Rights: Real World Application of Rights to Access, Rectification, Object, Erasure, and Data Portability' (2026) NDPC Journal 121; Dolapo Dorcas Oyawole, 'An Assessment of the Scope and Enforcement of Data Subject Rights under Nigerian Data Protection Regimes' (2025) Lawrit Journal of Law vol V issue II.

138 NDPA 2023, ss 24(3), 32 and 34–38; GAID 2025, arts 12–13, 36 and 45.

139 Nigeria Data Protection Act 2023, s 40(1), (2), (4), (8); General Application and Implementation Directive 2025, art 34; Bernold Nieuwesteeg and Michael Faure, 'An Analysis of the Effectiveness of the EU Data Breach Notification Obligation' (2018) 34(6) Computer Law & Security Review 1232.

4.6.4 The NDPC should complete its investigation into the alleged unauthorised disclosure of Emeka Ike's voter-registration information by INEC and publish an appropriate outcome, subject to legitimate confidentiality, security and due-process considerations. The investigation should determine, among other matters, whether a personal-data breach occurred; the categories and scope of personal data affected; the circumstances in which the information was accessed and disclosed; whether INEC complied with its obligations under section 40 of the NDPA; whether appropriate technical and organisational measures were in place to prevent unauthorised access or disclosure; and whether remedial measures are required. Where violations are established, the Commission should exercise its statutory enforcement powers and communicate the outcome in a manner sufficient to demonstrate regulatory accountability without unnecessarily disclosing further personal information. Such an outcome would serve both a remedial and systemic function. It would provide an authoritative determination of the circumstances surrounding the incident while clarifying for INEC, SIECs and other public-sector controllers how the NDPA's breach-management requirements apply to electoral data. It would also reinforce the principle that the public-sector status of an electoral institution does not immunise it from data-protection accountability.[140]

4.7 Capacity Building and Training for Electoral Officials

The operational challenges documented in respect of the SIECs, including reliance on temporary staff, the absence of permanent local government offices, and severe under-resourcing, mean that legislative and policy reform will have limited effect unless accompanied by sustained capacity building. The following measures are recommended:

4.7.1 INEC and each SIEC should institute mandatory, role-specific data-protection training for all personnel who handle voter personal data, including permanent employees, temporary personnel, contractors and ad hoc election or registration officials whose duties involve the collection, verification, access, transmission or other processing of personal data. Particular emphasis should be placed on personnel directly involved in biometric registration and voter accreditation because errors or unauthorised disclosures at these points occur at the interface between the electoral body and the data subject.[141] Training should cover the principles of lawful and fair processing, data minimisation, confidentiality, secure handling of biometric information, data-subject rights, incident and breach reporting, and escalation to the DPO. Given the recurrent use and turnover of ad hoc electoral personnel, training should not be treated as a one-off compliance exercise. INEC and SIECs should require completion of appropriate data-protection training before personnel are authorised to undertake functions involving voter data and should refresh that training before each major electoral cycle or whenever material changes are made to the technologies or procedures used to process voter data.[142]

4.7.2 The NDPC should extend the capacity-building approach reflected in its engagement with INEC to SIEC personnel and, where appropriate, to third-party technology vendors and processors participating in the electoral data ecosystem. This should include specialised training in privacy-information management and information-security standards, including ISO/IEC 27701 and ISO/IEC 27001 where proportionate and appropriate to the functions performed. The objective should not necessarily be to require every electoral employee or vendor to obtain ISO certification, but to establish a consistent baseline of competence concerning privacy governance, information security, risk management, access controls, incident response and accountability throughout the processing chain.

4.7.3 This recommendation is particularly important where voter data move between electoral bodies and technology providers. A controller's compliance cannot be secured solely through training its own employees where processing is also undertaken by external processors and vendors. Training requirements should therefore be incorporated, where appropriate, into procurement, data-processing agreements and vendor due-diligence procedures.

4.7.4 The NDPC, in collaboration with FOSIECON, should develop a simplified electoral data-protection compliance toolkit specifically designed for SIECs.[143] The toolkit should translate the requirements of the NDPA and GAID into practical, sequential steps capable of implementation by electoral bodies with limited financial, technological and human resources. It should contain model privacy notices, lawful-basis assessment forms, basic Records of Processing Activities templates, data-processing agreement checklists, data-subject request procedures, breach-reporting checklists, DPIA screening questions, minimum security-control requirements and a basic compliance calendar. The toolkit should adopt a proportionate implementation model rather than a reduced legal standard. In other words, limited institutional capacity should determine the form and complexity of the compliance mechanism, but should not exempt an SIEC from the substantive duties imposed by the NDPA.

Footnotes

140 Nigeria Data Protection Act 2023, ss 40, 46–48

141 Gabriel Ayodeji Obimuyiwa, Leila Leonardovna Salekhova and Blessing Adejoke Owolabi, 'Building a Culture of Data Protection: A Pedagogical Basis for Data Privacy Literacy in Nigerian Universities' (2026) NDPC International Journal of Data Privacy and Protection 111.

142 Nigeria Data Protection Act 2023, ss 24(3), 32 and 40; General Application and Implementation Directive 2025 (GAID 2025), arts 30 and 46

143 FOSIECON describes itself as the umbrella body for the 36 SIECs, while individual SIECs operate independently of INEC. This makes a coordinated capacity-building mechanism particularly appropriate. FOSIECON has also publicly acknowledged the institutional challenges facing SIECs and its objective of promoting more efficient election administration across the state commissions. See Isa Abdulsalami Ahovi, 'SIECs must be independent, not state government tools — FOSIECON' The Guardian Nigeria (21 May 2025) (reporting the FOSIECON National Chairman's statement that the organisation's mission is to promote efficient election administration in all 36 SIECs and acknowledging the 'plethora of daunting challenges' confronting SIECs). < https://guardian.ng/politics/siecs-must-be-independent-not-state-government-tools-fosiecon/?utm_source> Accessed 13 September 2026

The approach would enable smaller electoral bodies to identify and prioritise minimum essential controls while progressively developing more sophisticated governance arrangements.

4.7.5 Any legislative reform designed to strengthen the financial autonomy of SIECs should expressly recognise data-protection compliance as a core component of electoral administration and provide for an appropriate, ring-fenced allocation for its implementation. Such funding should support, according to the risk profile and processing activities of each SIEC, the appointment and continuous professional development of a qualified Data Protection Officer, secure storage and transmission infrastructure, encryption and access-control mechanisms, staff training, DPIAs, compliance audits, breach-response capabilities and other appropriate technical and organisational measures. The objective should not be to prescribe a uniform expenditure level for every SIEC, but to ensure that each Commission has sufficient resources to discharge the data-protection obligations applicable to its processing activities. Financial autonomy without corresponding resources for information governance may leave SIECs formally subject to the NDPA while lacking the practical capacity to comply with it. Accordingly, proposed funding arrangements should require SIECs to identify data-protection expenditure within their annual compliance and operational plans and to account for the implementation of material privacy and security controls.

4.8 Public Awareness and Voter Education on Data Rights

Ultimately, the enforceability of data subject rights depends on voters being aware that such rights exist. The following measures are recommended:

4.8.1 INEC and the SIECs should integrate data-protection and voter-privacy education into their existing continuous voter registration and public enlightenment programmes rather than treating data rights as a separate, stand-alone compliance initiative. Voters should be informed, in accessible language, not only about how to register and participate in elections but also about the personal and biometric information collected from them, the purposes for which it is processed, the institutions and categories of third parties that may have access to it, the principal safeguards applicable to it, and the mechanisms available for exercising their data-subject rights and making complaints.[144] This approach would embed privacy awareness within the point at which voters actually interact with electoral institutions and provide personal information. It would also give practical effect to the transparency and information obligations imposed by the NDPA and help voters understand that the submission of personal and biometric information to an electoral body does not extinguish their rights as data subjects.

4.8.2 INEC and each SIEC should produce simplified, multilingual and accessible voter-privacy materials for distribution at registration centres and through their websites, social-media channels, radio and other public-enlightenment platforms.[145] At a minimum, the materials should explain in plain language the categories of personal and biometric data collected during voter registration and accreditation, the purposes for which the information is processed, the principal safeguards applicable to it, the circumstances in which it may be shared, the rights available to voters, and the channels through which privacy-related complaints or requests may be submitted. The materials should be designed for voters with different levels of literacy and digital access and should, where appropriate, be available in English and relevant Nigerian languages. Digital FAQs should complement, rather than replace, physical materials at registration centres so that lack of internet access does not become a barrier to understanding data-protection rights.

4.8.3 INEC, the SIECs and the NDPC should establish structured channels of engagement with civil-society, civic-technology and digital-rights organisations working on electoral integrity, privacy and data protection. Such organisations can contribute to voter education, community outreach, independent technical and legal expertise, identification of emerging privacy risks and dissemination of accessible information to communities that may be difficult for electoral institutions to reach directly.[146] Collaboration should operate within clearly defined terms of reference and should complement, rather than substitute for, the statutory supervisory and enforcement functions of the NDPC or the constitutional responsibilities of electoral bodies. Particular consideration should be given to organisations with demonstrated experience in privacy litigation, data-protection advocacy and electoral accountability. Their participation can provide an additional channel through which recurring concerns affecting voters are identified and communicated to electoral institutions and regulators.

4.8.4 The NDPC and electoral bodies should introduce periodic public reporting on the state of voter-data protection within the electoral system. Such reporting should, in aggregate and appropriately redacted form, provide information on the number and general categories of reported personal-data breaches, the

Footnotes

144 Precious Okeoghene Okoh, Audience Knowledge, Attitudes and Practices of the 2023 Nigerian Data Protection Act (Covenant University 2025).

145 Nigeria Data Protection Act 2023, ss 24(1)(a) and 27(1), (3); GAID 2025, art 27.

146 Usman Gayam Usman and Muhammad Bello BabanUmma, 'Impact of Social Media on Voters Education in 2023 General Election in Nigeria' (2025) 11(8) Journal of Political Science and Leadership Research 164

number of data-subject requests and complaints received and resolved, compliance-audit participation and broad findings, material remediation measures undertaken, and significant data-protection initiatives implemented during the reporting period.[147] Where deficiencies are identified, reports should indicate whether corrective action has been completed, remains outstanding, or is subject to further regulatory intervention. Publication should be sufficiently detailed to enable voters, civil-society organisations and other stakeholders to assess whether electoral institutions are progressively improving their data-protection practices, but should exclude personal information, security-sensitive technical details and information whose disclosure could facilitate further compromise of electoral systems. Periodic reporting would transform data protection from an essentially internal compliance matter into an observable component of electoral accountability. It would also provide a cumulative record against which improvements in voter-data governance can be assessed over successive electoral cycles.

Taken together, these recommendations are directed at closing the gap between the NDPA's formal guarantees and the electoral ecosystem's operational reality. They proceed from the premise, borne out by the findings in this study, that compliance driven by litigation and reputational pressure, as exemplified by INEC's response to the privacy policy suit and its handling of the Emeka Ike breach, is an inadequate foundation for the protection of the personal and biometric data of over 94 million Nigerian voters. A shift towards proactive regulatory oversight, institutionalised privacy governance within electoral bodies, and an informed electorate is necessary if Nigeria's data protection framework is to keep pace with the scale and sensitivity of its electoral data processing, particularly as the country approaches the 2027 general elections.

Footnotes

147 Nigeria Data Protection Act 2023, ss 24(3), 40 and 48; GAID 2025, arts 10, 27, 34 and 48.

CHAPTER 5
CONCLUSION

DRLIDF
DRLIDF
DRLIDF
DRLIDF

5.1 Summary of Findings

This study set out to assess the compliance of Nigeria's electoral bodies, principally the INEC and the 36 SIECs, with the transparency, accountability, and data subject rights obligations imposed by the NDPA and its GAID. The findings, taken as a whole, establish that compliance across the electoral ecosystem is not merely uneven but structurally deficient.

At the national level, INEC, notwithstanding its status as the custodian of a biometric and demographic database of over 94 million registered voters and its consequent classification as a data controller of major importance, was found to have operated without any privacy policy on its official website until compelled to do so by litigation. Even the privacy policy subsequently published was shown to address only incidental website interactions, such as cookies, enquiries, and recruitment, while remaining silent on the Commission's principal processing activity: the collection of biometric data through the Continuous Voter Registration system and its use within the Bimodal Voter Accreditation System (BVAS) and the INEC Result Viewing Portal (IReV). INEC was further found not to have published the contact details of its Data Protection Officer, contrary to the mandatory requirement in Article 11(2) of the GAID.

At the subnational level, the assessment of all 36 SIECs against a five-indicator transparency framework revealed an even more pronounced deficit. The overwhelming majority of SIECs maintain no independent website, no verifiable digital presence beyond fragmented state government portals, and, in every single case examined, no identifiable privacy policy. This is not a case of partial or inconsistent compliance; it is the near-total absence of the transparency architecture that the NDPA presupposes, notwithstanding that SIECs process substantial volumes of voter, staff, and candidate personal data.

The study also examined the electoral bodies' compliance with accountability obligations under the NDPA, including the filing of annual Compliance Audit Returns. While the NDPC's own reporting shows a marked increase in filings and compliance revenue across the economy generally, no publicly available evidence was found of any audit filing, disclosure, or enforcement action involving INEC, the SIECs, or registered political parties. The compliance status of the institutions responsible for the country's most sensitive citizen database therefore remains, on the evidence available, indeterminate.

Finally, the case study of the Emeka Ike voter data leak was used to test the electoral ecosystem's practical handling of a live breach against the three-part obligation in Section 40 of the NDPA: notification of the NDPC within 72 hours, communication with affected data subjects where the breach poses a high risk to their rights, and comprehensive documentation of the breach and remedial measures taken. INEC's conduct was found to fall short on each limb. The Commission's acknowledgment of the breach followed public exposure rather than preceding it, no evidence emerged of timely or public confirmation of NDPC notification, no direct communication with the affected data subject was shown to have occurred, and no breach documentation was made available to the public. The absence of any visible NDPC enforcement response to this episode further suggests a broader deterrence gap in the enforcement of the NDPA against public institutions.

Underlying each of these findings is a common thread identified throughout this study: where electoral bodies have taken any meaningful compliance step, whether INEC's publication of a privacy policy or the initiation of the NDPC-INEC partnership on ISO 27701 training, that step has tended to follow litigation, public pressure, or a breach, rather than proactive institutional design. Compliance in Nigeria's electoral data protection ecosystem is, at present, reactive rather than embedded.

5.2 Implications for Democratic Governance and Electoral Integrity

The deficiencies documented in this study carry implications that extend well beyond technical non-compliance with a regulatory statute. Personal data processing by electoral bodies sits at the intersection of two constitutional values: the right to privacy guaranteed under Section 37 of the Constitution, as judicially extended to personal data by the Court of Appeal, and the right to participate in free and credible elections. Where an institution holding biometric and demographic data on the overwhelming majority of the adult population cannot demonstrate that it safeguards that data transparently, securely, and accountably, both values are placed at risk simultaneously.

First, the absence of demonstrable data protection compliance threatens public trust in the electoral process itself. Voters who are required, as a precondition of exercising their franchise, to surrender fingerprints and facial biometrics are entitled to assurance that this data will not be misused, leaked, or exploited for purposes unconnected with the electoral mandate. The Emeka Ike episode, and the public reaction it generated, illustrates how a single, poorly managed breach can crystallise broader anxieties about the safety of voter data and, by extension, about the institution entrusted with administering elections.

Second, the near-total absence of privacy governance infrastructure across the SIECs raises a distinct but related concern for the integrity of subnational democratic processes, including local government and area council elections that fall outside INEC's direct purview. If data protection compliance is allowed to track institutional capacity so closely that better-resourced federal bodies comply only under litigation pressure while state-level bodies do not comply at all, the practical protection available to a voter's personal data becomes a function of geography rather than a uniformly guaranteed right, which sits uneasily with the constitutional character of the privacy guarantee.

Third, the unresolved question of the lawful basis for mandatory biometric collection, canvassed in this study, has a bearing on electoral legitimacy beyond data protection law narrowly construed. If the public interest and legal obligation bases identified in this study are correct, as this study finds them to be, that conclusion should be affirmatively and transparently communicated to voters rather than left to inference, since public confidence in the lawfulness of biometric registration is itself a component of confidence in the electoral process.

Fourth, the absence of visible NDPC enforcement against electoral bodies, despite the scale and sensitivity of the data involved, risks establishing an implicit hierarchy of accountability in which powerful public institutions are treated as de facto exempt from a regime that applies in principle to all data controllers. Left unaddressed, this dynamic could undermine the credibility of Nigeria's data protection framework more broadly, extending well beyond the electoral sector, since regulatory forbearance toward one category of powerful controller invites scepticism about the framework's application to others.

Taken together, these implications suggest that data protection compliance in the electoral sphere is not a peripheral, technical concern but a constitutive element of electoral integrity itself. As Nigeria approaches the 2027 general elections, the credibility of the process will depend not only on the accuracy of the voter register and the reliability of BVAS and IReV, but on whether the millions of citizens whose biometric and personal data underpin that register can trust that their information is being handled lawfully, transparently, and securely.

5.3 Final Reflections

This study has sought to move the conversation on voter privacy in Nigeria from the general observation that a data protection statute exists to a specific, evidence-based account of how that statute is being applied, and not applied, by the institutions charged with administering the country's elections. What emerges is a picture of a legal framework that is, on its face, reasonably comprehensive, set against an institutional practice that remains substantially reactive, uneven across tiers of government, and largely unaccompanied by visible regulatory enforcement.

None of this is to suggest that progress has been entirely absent. The eventual publication of a privacy policy by INEC, however belated and incomplete, the NDPC-INEC partnership on ISO 27701 training, and the growing willingness of civil society and the courts to hold electoral bodies to account, all indicate that the direction of travel is towards greater compliance rather than away from it. The task identified by this study is to accelerate and institutionalise that trajectory, so that compliance is designed into the electoral data ecosystem from the outset of each electoral cycle rather than extracted from it after the fact, whether by litigation, public outcry, or the exposure of a breach.

The recommendations advanced in Chapter Five, spanning legislative reform, strengthened NDPC oversight, institutionalised privacy governance, mandatory impact assessments, standardised transparency practices, responsive data subject rights mechanisms, capacity building, and public education, are offered as a coherent, mutually reinforcing programme rather than a menu of isolated interventions. Their common objective is to ensure that the constitutional guarantee of privacy under Section 37, and the statutory guarantees under the NDPA and the GAID, translate into lived protection for the tens of millions of Nigerians whose most sensitive personal data now underpins the machinery of their democracy.

Ultimately, the legitimacy of any electoral system rests on the confidence of the electorate, not only in the count of votes but in the custody of the information that makes each vote possible to cast and to verify. Voter privacy and electoral transparency, this study concludes, are not competing values to be traded off against one another but complementary pillars of the same democratic edifice. Reinforcing one without the other will leave that edifice standing on an incomplete foundation as Nigeria moves toward its next general elections.

VOTER PRIVACY AND UMPIRES' TRANSPARENCY: AN ASSESSMENT OF THE ELECTORAL BODIES' COMPLIANCE WITH THE NIGERIA DATA PROTECTION ACT (NDPA) 2023

Digital Rights Lawyers Initiative

Luminate