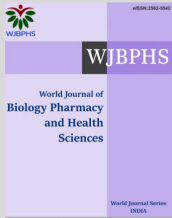




World Journal of Biology Pharmacy and Health Sciences
eISSN: 2582-5542
Cross Ref DOI: 10.30574/wjbphs
Journal homepage: <https://wjbphs.com/>



(RESEARCH ARTICLE)



AUTOMATED NDPA COMPLIANCE TOOLKIT FOR ARTIFICIAL INTELLIGENCE-DRIVEN STUDENT MANAGEMENT SYSTEMS IN NIGERIAN UNIVERSITIES

Jude Chijindu Chukwuemeka *

Miva Open University, Abuja, Nigeria.

* Corresponding Author

ORCID Details

Jude Chijindu Chukwuemeka: <https://orcid.org/0009-0001-8369-9114>

World Journal of Biology Pharmacy and Health Sciences, 2026, 28(01), 021–025

Publication history: Received on 30 August 2026; revised on 05 October 2026; accepted on 07 October 2026

Article DOI: <https://doi.org/10.30574/wjbphs.2026.28.1.0497>

Copyright © 2026 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0

ABSTRACT

Artificial intelligence has become a central pillar of institutional management in Nigerian higher education, processing massive volumes of student data for admissions, predictive analytics, and attendance management. However, this data-intensive transformation operates under the strict oversight of the Nigeria Data Protection Act (NDPA) of 2023. Despite these legal obligations, empirical evidence reveals a systemic governance deficit, characterized by bundled consent, unlawful cross-border data transfers, and automated decision-making without human oversight. This project aimed to design, develop, and evaluate an Automated NDPA Compliance Toolkit to systematically detect and remediate compliance violations within artificial intelligence-driven Student Management Systems. Design Science Research was adopted as the primary methodology, supported by documentary analysis and comparative technology assessment. The developed toolkit features a three-layer architecture utilizing Python, FastAPI, PostgreSQL, and React.js, operationalizing the NDPA into 25 executable checks across six compliance modules. Testing was conducted using a simulated non-compliant institution and a compliant control system. The toolkit successfully identified all planted violations in the non-compliant system, assigning a compliance health index of 12 percent, while accurately passing all checks for the compliant system with a 100 percent score. The confusion matrix indicated 100 percent detection accuracy and specificity. The findings establish that software can effectively bridge the gap between statutory requirements and practical implementation by translating legal provisions into verifiable technical controls.

Keywords: Artificial Intelligence; Data Protection; Ndpa 2023; Regulatory Technology; Student Management Systems

1 INTRODUCTION

Artificial intelligence has evolved from a peripheral technological curiosity to a central pillar of institutional management in higher education globally. Within Nigeria's tertiary education landscape, this transformation is especially evident. Universities increasingly deploy artificial intelligence-based platforms to process massive volumes of student data, ranging from admissions screening and academic performance analytics to biometric attendance management and predictive dropout modeling. Operating under structural pressures, including a national student-to-

lecturer ratio of approximately 45:1, Nigerian institutions rely heavily on artificial intelligence to manage administrative complexity and identify at-risk students early.

However, this rapid and data-intensive digital transformation now operates under the strict oversight of the Nigeria Data Protection Act (NDPA) of 2023. Enacted on 12 June 2023 and administered by the Nigeria Data Protection Commission (NDPC), the NDPA imposes binding obligations on all entities that collect, process, or store the personal data of Nigerian citizens. Key provisions directly applicable to university systems include the requirement for a lawful basis for all data processing, specific and informed consent, mandatory Data Protection Impact Assessments (DPIAs) for high-risk activities, and the right for students not to be subject to solely automated consequential decisions.

Despite the clarity of these legal obligations, empirical evidence reveals a systemic governance deficit across Nigerian universities. A survey found that fewer than 12 percent of Nigerian public universities had appointed a qualified Data Protection Officer as of January 2024. Six specific compliance failures characterize the current landscape: bundled consent practices that force students to accept profiling to access core services; data maximization where predictive models ingest unnecessary sensitive variables; a deficit of accountability lacking qualified oversight; inadequate security measures lacking encryption and audit logs; automated decision-making without human review; and unlawful cross-border data transfers to foreign servers.

The core problem is not merely a lack of regulatory awareness, but the absence of automated, institution-facing tools that can translate the NDPA's legal obligations into systematic, real-time technical checks in operational systems. Current compliance efforts remain largely paper-based, utilizing drafted policy documents and committee minutes while underlying architectures continue to process student data in ways that structurally violate the Act. Therefore, the aim of this project is to design, develop, and evaluate an Automated NDPA Compliance Toolkit that enables Nigerian universities to systematically detect, assess, report, and remediate NDPA 2023 compliance violations within their student management systems.

2 MATERIAL AND METHODS

This project adopted Design Science Research (DSR) as the overarching methodology. DSR is particularly well-suited to projects whose core contribution is the creation of an innovative artifact intended to solve an identified real-world problem. The methodology encompasses six stages: problem identification, definition of solution objectives, design and development, demonstration, evaluation, and communication. Within this framework, three complementary qualitative research methods were utilized to generate the necessary evidence for the toolkit's design: documentary analysis of the NDPA 2023, comparative technology analysis of global compliance platforms, and secondary data analysis of existing empirical studies on data governance in Nigerian higher education.

2.1 System Architecture and Module Design

The system architecture of the Automated NDPA Compliance Toolkit organizes its components into three interconnected layers. Layer 1 functions as the Entry Point, managing the connection to target systems through a Multi-System Registry and a Pre-Scan Validation Gate. Layer 2 operates as the Processing Core, executing the substantive compliance assessment functions across six specialized modules operating in parallel, followed by a Central Aggregation Engine that calculates institutional compliance indices. Layer 3 represents the Output Layer, delivering tailored reporting interfaces for Data Protection Officers, regulatory authorities, and students.

Table 1: Summary of NDPA 2023 Provisions Applicable to the Toolkit Modules

NDPA Section	Core Obligation	Toolkit Module
Section 24, 26	Lawful basis and specific, freely given consent	Consent Verification
Section 26(2)(b)	Limiting data collection to necessary variables	Data Minimisation
Section 29, 32	DPIA execution and qualified DPO appointment	Accountability Validation
Section 39	Technical and organisational security measures	Integrity and Security
Section 41	Right against solely automated decisions	Human Oversight
Section 43, 45	Prohibition on unlawful cross-border transfers	Cross-Border Transfer

The implementation technology stack was selected based on fit for purpose, contextual appropriateness within the Nigerian university operating environment, and long-term stability. The toolkit was developed using Python 3.11 as the

primary programming language due to its extensive ecosystem for HTML parsing and API integration. FastAPI was utilized for the backend framework to natively support asynchronous parallel processing of the compliance modules. PostgreSQL 15 served as the relational database, providing native JSON column support to store structured module outputs. The deployment infrastructure relied on Docker containerization running on Ubuntu Server 24.04, with Nginx acting as a reverse proxy.

Table 2: Comparative Design Specifications of the Compliance Modules

Module	Purpose	Key Implementation Logic
Consent Verification	Verify specific, informed, freely given consent	Bundling detection, coercion test, notice completeness audit
Data Minimisation	Verify only necessary data variables are processed	Justification coverage thresholds, sensitive category screening
Accountability Validation	Verify DPO appointment and DPIA currency	DPO qualification check, DPIA 12-month currency validation
Integrity and Security	Verify encryption, access control, and audit logging	Encryption at rest/transit verification, RBAC, tamper-evident logs
Human Oversight	Verify human review of consequential decisions	Review coverage ratio, auto-enforcement detection, contestation test
Cross-Border Transfer	Verify lawful transfer mechanisms for data leaving Nigeria	Jurisdiction detection, lawful mechanism verification

3 RESULTS

The evaluation of the toolkit was conducted through four structured testing methodologies: detection accuracy, specificity (negative testing), performance, and determinism. To facilitate this without violating the data privacy of live institutional systems, two simulated target systems were developed. 'University Beta' was constructed as a non-compliant target, deliberately populated with six specific NDPA violations corresponding to documented empirical practices. 'University Alpha' was developed as a fully compliant control system to test the toolkit's specificity and ensure it did not generate false positive alerts.

Table 3: Controlled Contrast Between the Non-Compliant Target and Compliant Control

NDPA Domain	University Beta (Non-Compliant)	University Alpha (Compliant Control)
Consent	One bundled checkbox; declining blocks registration; deficient privacy notice	Four granular checkboxes; declining does not block access; complete notice
Data Minimisation	47 variables collected; only 5 justified; sensitive data included	8 variables collected; all carry documented necessity justifications
Accountability	No DPO appointed; no DPIA ever conducted	Qualified DPO appointed; DPIA conducted 95 days prior to scan
Security	No encryption; shared admin accounts; unpatched critical vulnerabilities	AES-256 encryption; role-based access; zero unpatched vulnerabilities
Human Oversight	1,847 consequential decisions with zero human reviews	942 consequential decisions with 942 documented human reviews
Cross-Border	Data hosted in the United States; no Data Processing Agreement	Data hosted locally in Lagos, Nigeria; processing agreement in place

3.1 Detection Accuracy and Specificity Results

During the detection accuracy phase, all six compliance modules were executed against the non-compliant University Beta system. The toolkit successfully identified all six planted violations, resulting in a 100 percent detection rate with zero missed infractions. The institutional Compliance Health Index aggregated to 12 percent, resulting in an overall

'FAIL' verdict. The scan identified 12 distinct NDPA sections violated across 22 failed checks and automatically generated 21 prioritized remediation actions for the institution.

Conversely, during specificity testing against the compliant University Alpha system, every module passed. The toolkit successfully evaluated all 25 checks without triggering any false alarms or unwarranted remediation actions. The Compliance Health Index recorded 100 percent, yielding an overall 'PASS' verdict.

Table 4: Detection Accuracy Results Against University Beta

Planted Violation	Detecting Module	Verdict	Score
Bundled, coerced consent	Consent Verification	FAIL	20%
Data maximization (47 variables)	Data Minimisation	FAIL	33%
No DPO, no DPIA	Accountability Validation	FAIL	0%
Absent technical measures	Integrity and Security	FAIL	0%
No human oversight	Human Oversight	FAIL	0%
Unlawful cross-border transfer	Cross-Border Transfer	FAIL	17%

The performance testing demonstrated high operational efficiency. Across five repeated runs, a full 25-check scan of University Beta averaged 0.017 seconds, while University Alpha averaged 0.015 seconds, translating to over 1,500 compliance checks executed per second. Determinism testing verified that identical inputs consistently yielded identical compliance verdicts across multiple executions, confirming the reliability necessary for regulatory reporting tools.

Table 5: Confusion Matrix Across Twelve Module-Level Observations

Test Condition	Predicted FAIL	Predicted PASS
Actual violation present (Beta)	True Positives = 6	False Negatives = 0
Actual compliance present (Alpha)	False Positives = 0	True Negatives = 6

4 DISCUSSION

The evaluation results confirm that NDPA requirements can be successfully translated into automated technical checks that provide clear, evidence-based, and actionable results for institutions. A critical finding is the toolkit's capability to differentiate between varying states of compliance rather than executing a rigid, universally failing assessment. The strict AND aggregation logic effectively separates legality from remediation progress. The verdict answers the binary legal question by escalating to the most severe finding, while the percentage score answers the progress question, allowing a Data Protection Officer to track incremental remediation improvements without falsely claiming full statutory compliance. By generating prioritized remediation registers tied to specific NDPA provisions, the toolkit transforms a diagnostic audit into a structured operational work plan.

5 CONCLUSION

The Nigeria Data Protection Act 2023 possesses legal authority but severely lacks practical enforcement mechanisms at the technical level within university environments. A law that exists solely on paper, without scalable means of verification, remains theoretical rather than operational. The central premise of this project is that software can bridge the gap between statutory requirements and practical implementation. The empirical results successfully validated this premise, demonstrating that the NDPA's provisions can be operationalized as automated technical controls.

By translating twelve legal provisions into twenty-five evidence-based checks, the Automated NDPA Compliance Toolkit successfully distinguishes between compliant and non-compliant systems with 100 percent precision within a controlled testing environment. For Data Protection Officers, the toolkit translates unbounded legal exposure into a structured remediation plan. For regulators, it demonstrates the viability of supervisory tools capable of systematically assessing the compliance status of numerous institutions at scale. Ultimately, the integration of regulatory technology

within educational institutions ensures that data protection obligations are no longer relegated to static policy documents, but are actively enforced as verifiable properties of the technological infrastructure.

STATEMENTS ON COMPLIANCE WITH ETHICAL STANDARDS

Acknowledgments

The author gratefully acknowledges the institutional and academic support provided by Miva Open University for the research and manuscript preparation. Special appreciation is extended to Dr. Ugochi Okengwu for providing invaluable technical mentorship, guidance, and supervision throughout the development of the Automated NDPA Compliance Toolkit.

Disclosure of conflict of interest

The author declares that there is no conflict of interest regarding the publication of this manuscript.

REFERENCES

- [1] Bello T, Afolabi O. Trust deficit in AI-powered academic decision systems: Evidence from Nigerian postgraduate students. *African Journal of Educational Management*. 2022; 29(2):112-131.
- [2] Chukwuemeka JC. AI governance and the Nigeria Data Protection Act (NDPA): A framework for ethical student data management in Nigerian universities [Seminar Paper]. Miva Open University. 2026.
- [3] National Universities Commission (NUC). List of accredited universities in Nigeria. 2024.
- [4] Nigeria Data Protection Act. Official Gazette of the Federal Republic of Nigeria. 2023.
- [5] Nigeria Data Protection Commission (NDPC). Strategic roadmap and action plan (SRAP) 2023-2027. 2023.
- [6] Shokunbi O, Agbaje M, Ogu EC. Measuring Nigeria Data Protection Act (NDPA) 2023 compliance in Nigerian universities: A general compliance index and evidence of institutional decoupling. *FUDMA Journal of Sciences*. 2026; 10(6):5085-5095.
- [7] Cavoukian A. Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario. 2009.
- [8] Peffers K, Tuunanen T, Rothenberger MA, Chatterjee S. A design science research methodology for information systems research. *Journal of Management Information Systems*. 2007; 24(3):45-77.