

Webinar Report



Data Protection for **Ministries, Departments and
Agencies of Government**



About LawDigits

LawDigits is a technology, law and digital governance-focused organisation committed to helping businesses, government institutions and professionals navigate the rapidly evolving digital landscape.

We operate at the intersection of law, technology, data protection, artificial intelligence, cybersecurity and digital governance, providing practical solutions that help organisations understand their obligations, manage digital risks and responsibly adopt technology.

Through initiatives such as our **MDA Awareness Month**, professional communities, webinars, research and practical compliance resources, LawDigits seeks to contribute to the development of a more informed and responsible digital ecosystem in Nigeria.

See more on our website at www.lawdigits.com



DATA PROTECTION COMPLIANCE FOR GOVERNMENT MDAS

Understanding the Problems, Addressing Issues, and Delivering Solutions

SPEAKERS



Mr. Tokunbo Smith
Founder
Institute of Data Governance Nigeria



Dipo Ige
Team Lead
LawDigits

FREE WEBINAR
TECHNOLOGY LAW

29 Tuesday
September 2026
02:00pm - 03:00pm (WAT)
02:00pm - 03:00pm (GMT+1)



Copy the link to register or scan the QR Code
<https://forms.gle/yAto7hoD1dxW4hUU7>



SPEAKER PROFILE

MR TOKUNBO SMITH
Founder, Institute of Data Governance, Nigeria

Tokunbo Smith has been a pioneer in the development and promotion of data protection and privacy practice in Nigeria. T&Y Information Management Services Ltd (TYIMS) was one of the pioneer Data Protection Compliance Organisations (DPCOs) licensed by the National Information Technology Development Agency (NITDA) under Nigeria's earlier data protection regulatory framework.

He was also the first consultant to the Lagos State Government on Data Protection Compliance, supporting the development of institutional awareness and compliance approaches within the public sector. He was among the pioneers who promoted public awareness of data protection in Nigeria and was the first to celebrate World Data Privacy Day in Nigeria, helping to establish greater visibility for privacy and responsible data management.

He has contributed to the development of framework policies and regulatory initiatives of the Nigeria Data Protection Commission (NDPC) and NITDA, and has participated extensively in stakeholder consultations, professional engagements and policy-development activities relating to data protection and digital governance.



29 September 2024

TIME 2:00PM - 3:00PM

https://forms.gle/yAo7heD1dxW4h1UJ7





SPEAKER PROFILE

DIPO IGE
Team Lead, LawDigits

Dipo Ige is a legal practitioner specialized in Data Protection/Privacy Law, Cybersecurity and Artificial Intelligence Governance with vast experience in privacy litigations, data protection assessments, analysis, research as well as responsible AI development and deployment. He is an expert in rendering regulatory consultation services to both public and private actors on complex data matters, delivering privacy-driven strategic solutions and training. In the courts, Dipo has participated in major privacy and personal data related cases as a Partner in Equibridge Attorneys (EBA). He has also litigated matters involving the legal critique of data protection legislations and the role of regulators in the privacy space. Dipo holds a master's degree in International Human Rights Law with specialisation in privacy rights. He has experience as an implementer of the ISO 27001, ISO 42001, ISO 42005, NIST Framework, EU AI Act, Cybersecurity laws and the NDP-GAID 2025.

He is currently the Team Lead at LawDigits, a consultancy firm specialised in Privacy, Cybersecurity and Artificial Intelligence governance, doubles as the Director of Policy & Advocacy of the Data Privacy Lawyers Association of Nigeria (DPLAN) and the Team Lead at Sentient Innovation Lab (SIL).



29 September 2024

TIME 3:00PM - 3:30PM

https://forms.gle/yAo7heD1dxW4h1UJ7



Webinar Overview

The Data Protection for MDAs Webinar detailed the stipulated data protection mandates within the public sector as well as the security challenges, solutions and compliance strategies. These are the major themes discussed throughout the event;

Public Sector Data Challenges

Ministries, Departments & Agencies (MDAs) process large volumes of personal data while facing widespread staff/personnel ignorance, fragmented databases, and are still largely reliant on legacy paper systems.

Compliance and Vendor Management

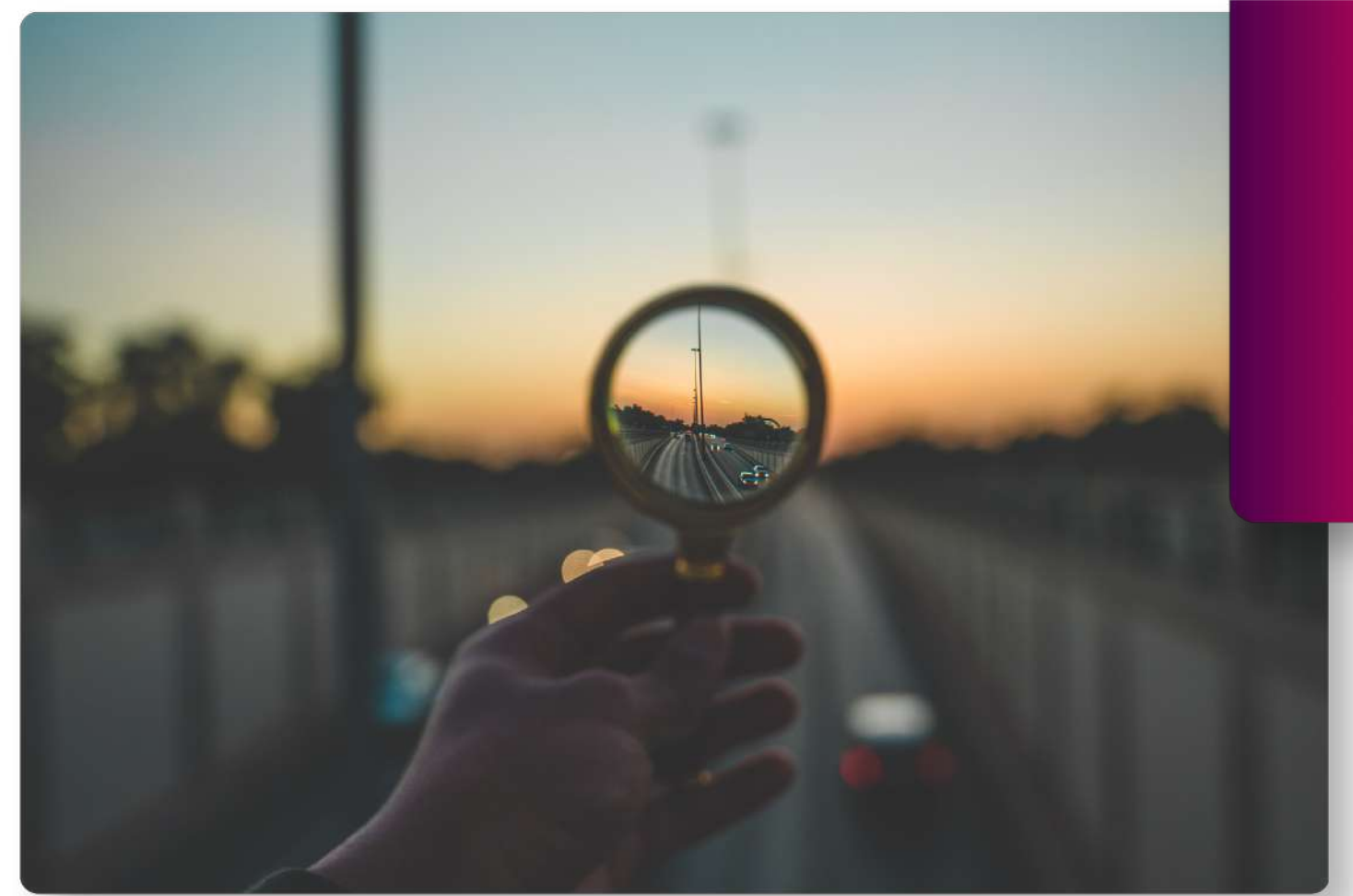
MDAs must secure annual budgets specifically for data protection compliance, appoint competent compliance organisations to vet and verify their compliance obligations, and they must enforce strict vendor safety assessments embedded within their third party onboarding practices.

Cybersecurity and Physical Security

The experts laid emphasis on MDAs adopting clear desk policies, educating personnel on personal liabilities including the liabilities of the Permanent Secretaries, Directors and Chief Executive Officers/Director General of MDAs. The experts also addressed fake scam applications, using unvetted flash drives within MDAs and best practices to reduce or mitigate data protection violations.

Procession

Gbamwuan iengem Jemima opened the webinar hosted by LawDigits, focusing on data protection for government ministries, departments, and agencies. Gbamwuan iengem Jemima noted that in July 2026, the secretary to the government of the federation issued a circular mandating all ministries, departments, and agencies to comply with the Data Protection Act 2023 and the guidelines on data protection. Gbamwuan iengem Jemima introduced the expert speakers Mr. Tokunbo Smith and Mr. Dipo Ige, highlighting that the core objective of the webinar is to examine the practical meaning of data protection, existing problems, and potential solutions for Ministries, Departments, and Agencies. The following are major points discussed;



① The Importance of Personal Data and Human Rights Risks

Dipo Ige explained that personal data represents individuals themselves including names, phone numbers, house and office addresses, and biometrics, without which human society and communication cannot function. He highlighted that exposure of personal data creates severe human rights risks and vulnerabilities, such as identity theft, unauthorized phone calls, kidnappers tracking targets, and criminals using stolen National Identification Numbers or Bank Verification Numbers to open bank accounts, obtain loans, or incur debt.

② Overview of Public Sector Data Protection Challenges

Mr. Tokunbo Smith stated that government Ministries, Departments, and Agencies process large volumes of personal data, including **citizen identity records, health information, tax and employment records, education and financial records, biometric data, immigration information, social welfare data, and closed-circuit television surveillance**. He identified the primary public sector challenges in Nigeria, including widespread ignorance, large-scale flat databases, sensitive and high-risk data processing, multiple uncoordinated databases, inter-agency data sharing inefficiencies, reliance on third-party service providers, legacy paper and electronic systems, cross-border data transfers, and the unregulated use of Artificial Intelligence that violates data minimization principles.

“Protect the People behind the Data”

3 Addressing Ignorance and Public Awareness

Addressing the problem of ignorance among Civil Servants and the public, Mr Smith recommended continuous training conducted by licensed Data Protection Compliance Organisations (DPCOs) rather than relying solely on awareness campaigns. He suggested tailoring private sector training using accessible language like Pidgin English for support staff, replacing vulnerable physical visitor registers with quick response code systems, and utilizing public graphics and billboards in major languages to educate citizens. He also made an example of using graphics to educate market women and the ease of comprehension . Mr. Dipo also noted the risk of document exposure, termed the **Akara dilemma**, where documents containing citizen data are improperly reused or discarded by MDAs.

4 Leadership Commitment and Consolidating Databases:

Mr Tokunbo Smith noted that **limited leadership commitment** is a major barrier, where data protection is improperly treated as solely a Data Protection Officer's responsibility rather than an institutional duty. To address multiple fragmented databases and leadership gaps, Mr Smith recommended starting with a sectoral approach to build robust databases and not committing to the change at once, securing executive sponsorship from Chief Accounting Officers (such as Permanent Secretaries or Director-Generals), and establishing a Data Protection Governance Committee equipped with management reporting and institutional key performance indicators. He believes that this will invigorate the MDAs to comply with the law and ensure sanctions in the event of gross and evident non-compliance.



Ever heard of the “Akara Dilemma?”



“Which is a better MDA risk between getting burnt by Fire and Hacking?”

⑤ Budgeting and Financial Resourcing for Compliance:

Mr. Smith identified **insufficient funding** as a core challenge restricting resources for MDA trainings, audits, and compliance technology. To resolve funding deficits, he recommended establishing an annual data protection compliance budget linked to identified risks and statutory obligations, insisting that each Ministry, Department, and Agency must independently appoint their own Data Protection Compliance Organisation (DPCO) and secure independent budget approvals rather than relying on a centralised ministry-wide budgets.

⑥ Managing Legacy Information Systems:

Discussing the continued reliance on paper records within Ministries, Departments, and Agencies in 2026, Mr. Tokunbo Smith asserted that legacy information systems present significant vulnerability risks compared to electronic databases with proper backups. He recommended establishing a mandatory deadline of six to nine months for MDAs to convert paper information to electronic formats, provided that necessary funding is officially supplied by the government and the required experts are consulted to handle the transition.

⑦ Managing Third-Party Vendors and Procurement Risks:

Mr. Smith explained that MDAs frequently collaborate with Third-party Service Providers and Private Vendors, which creates compliance risks if Vendors are unregulated. He detailed that procurement departments often prioritize lowest costs over safety and vulnerability assessments. To mitigate vendor risks, Mr Smith recommended that MDAs must maintain a vendor database, mandate data protection compliance as a prerequisite for registration through procurement, and ensure procurement personnel receive proper data protection training. He also warned that non-compliance results in severe consequences, including reputational damage, career destruction for Chief Executive Officers and government employees, cash flow disruptions, and regulatory fines.

⑧ Public-Private Collaboration and System Vulnerabilities:

Law Digits highlighted a current court case involving cybersecurity experts who uncovered compromised National Identification Number slips of high-ranking government officials, illustrating systemic vulnerabilities ([00:54:17](#)). Law Digits asked whether public agencies should rely on private sector experts to resolve data security issues, to which Tokunbo Smith responded that ministries, departments, and agencies must engage private consultants and cybersecurity experts because public agencies cannot operate as isolated entities, though personal interests and non-committed leadership often obstruct these collaborations ([00:55:32](#)).



Regulatory Enforcement and Accountability for Government Agencies:



During the question-and-answer session, Mr. Abdullah Tijani asked how the National Data Protection Commission (NDPC) can ensure MDAs comply with the law, noting that enforcement actions are more commonly observed against private companies. Mr. Tokunbo Smith responded that the National Data Protection Commission has taken enforcement actions against entities such as the Corporate Affairs Commission (CAC), and explained that future accountability measures will target Chief Accounting Officers of the MDAs such as Permanent Secretaries and Director-Generals. He said it might even be by removing them from their positions and damaging their reputations as a failed leader because of the implications of data breaches in their tenure, rather than merely relying on government funds to pay regulatory fines.

NDPC Compliance Metrics and MDA Digitization:



Olamiji Ogun raised questions regarding national importance and the policy context surrounding the government mandate for the digitization of all Ministries, Departments, and Agencies before December 31st of the previous year. He inquired about specific audit mechanisms and metrics deployed by the National Data Protection Commission to verify compliance, the percentage of MDAs with formally registered Data Protection Officers, and support mechanisms for underfunded agencies.

Mr. Tokunbo Smith addressed Olamiji Ogun's inquiries by noting that external proposals regarding compliance dashboards have been submitted to the NDPC, which welcomes strategies and tests ideas before implementation. Tokunbo Smith emphasized the necessity of establishing a solid policy foundation to avoid public criticism if errors occur, noting that government mandates for MDAs also carry implications for the private sector, similar to how minimum wage policies affect both government and private entities. He admonished that both sides of the coin must be put into consideration.

Mitigating Physical Record Vulnerabilities and Ensuring Data Security:



Oladapo Omitogun highlighted the rampant issue of physical paper records containing sensitive personal data stacked openly in offices across various MDAs that lack digital understanding, asking how to mitigate these vulnerabilities while awaiting government funding and support. Mr. Tokunbo Smith advised that individuals should educate contact persons on personal liabilities, such as the risk of jail time if sensitive records are misused, and promote a clear desk policy rather than waiting entirely for the government or the NDPC. To illustrate security risks, Mr. Smith shared past experiences from training sessions, including a visit to the Central Bank of Nigeria years back where he demonstrated vulnerability by discussing flash drive risks with the Human Resources Director, and another instance where a participant returned a strong room key after learning about the possible risks and liabilities. Mr Dipo reinforced this by referencing the real-life Stuxnet operation where a flash drive was used to shut down an Iranian nuclear facility by USA and Isreal, emphasizing that awareness, responsiveness, and proper protocol regarding flash drives and open documents are critical for all government MDAs.



Closing Remarks and Future Collaboration:

Mr. Dipo Ige concluded the webinar by directing participants to reach out via email, website, or LinkedIn for further questions, and expressed an interest in ongoing collaborations. Mr. Tokunbo Smith expressed gratitude for the opportunity to share experience and suggested holding similar educational sessions on a quarterly basis.

The session was thereafter adjourned.

Key Recommendations



Training and Awareness:

Conduct continuous training via licensed Data Protection Compliance Organizations using accessible language and public billboards rather than relying solely on government awareness campaigns.



Governance and Budgets:

Secure executive sponsorship from Chief Accounting Officers, establish Data Protection Governance Committees, and set Independent Annual Compliance Budgets for each MDA.



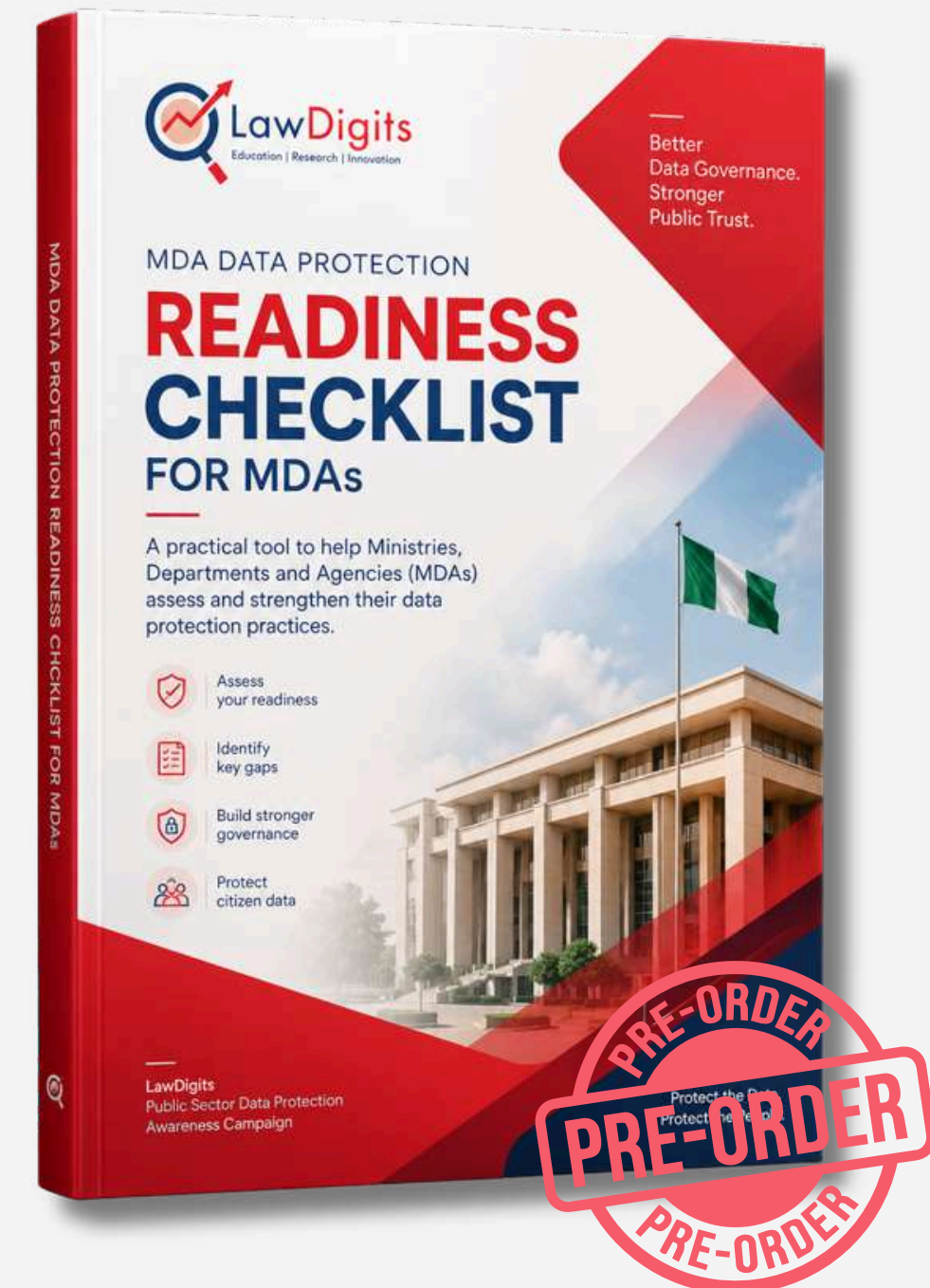
Physical Security:

Replace vulnerable physical Visitor Registers with QR code systems and enforce Clear Desk Policies to prevent unnecessary document exposure.



Collaboration:

MDAs should engage private sector Cybersecurity Experts and Consultants to address systemic vulnerabilities and track scam applications or fake lookalike websites.





Thank You!



Keep learning about Data Protection in Real Life



www.lawdigits.com | admin@thelawdigits.com