FEDERAL REPUBLIC OF NIGERIA

NIGERIA DIGITAL IDENTIFICATION FOR DEVELOPMENT PROJECT

TERMS OF REFERENCE FOR LEGAL CONSULTANCY SERVICES FOR THE DRAFTING OF A COMPREHENSIVE DATA PROTECTION LEGISLATION FOR THE FEDERAL GOVERNMENT OF NIGERIA

1. BACKGROUND

1. Of the 187 million living in Africa's most populous country, only about 30% have had their births registered - this figure drops to 19% in rural areas and to 7% within the poorest quintile of the population. Less than 50% of residents have any form of ID card, whilst only 9% of individuals have a national ID number (NIN).

2. Nigeria hosts a fragmented ID landscape which incurs significant costs on the Federal Government (FGN). Over 13 government agencies (National Identity Management Commission, National Population Commission, Central Bank of Nigeria, Independent National Electoral Commission, Nigerian Communications Commission and others) and at least 3 state agencies offer ID services in Nigeria. Many of these agencies capture biometrics and issue ID cards independently without data links with other systems, resulting in duplication and sub-optimal utilization of scarce resources.

3. The FGN has indicated a strong desire to harmonize the existing identification ecosystem towards developing a foundational identification platform which can be leveraged to improve service delivery. A Strategic Roadmap for Developing Digital Identification in Nigeria was prepared with the support of the World Bank Group, and highlighted the need for a minimalist, foundational, and eco-system-based approach to identification in the country. The Roadmap was endorsed by the Harmonization Committee on January 31, 2018, and by the Federal Executive Council (FEC) in September 2018.

4. Consequently, the FGN applied for a credit from the World Bank to increase the number of persons in Nigeria who have government-recognized proof of unique identity that enables them to access services. The Project will be implemented by a Project Implementation Unit (PIU) in the National Identity Management Commission (NIMC) and an Ecosystem Coordination Strategic Unit (ECSU) in the Office of the Secretary to the Government of the Federation (OSGF) under the oversight of a Project Ecosystem Steering Committee (PESC).

5. The project has been divided into four components, namely, Strengthening the Legal and Institutional Framework, Establishing a Robust and Inclusive Foundational ID System, Enabling Access to Services through IDs and the Project Management and Stakeholder Engagement.

6. As part of the Nigeria ID4D project preparation, a legal and regulatory review was undertaken in 2018 to assess the readiness of the existing legal and regulatory enabling environment in Nigeria to support the national digital identification system and the broader digital economy. The review focused on the legal and regulatory enabling environment

under each of the following themes: governance arrangements; flow of information / data; the support and promotion of mutual recognition and interoperability of identification credentials; transparency; individual privacy rights; digital authentication, and legal recognition of online transactions; non-discrimination; and specific implementation risks. The legal review provided a readiness assessment of legal instruments and processes, identified potential implementation risks, and recommended possible reforms and risk mitigation measures.

7. The legal and regulatory assessment and the recommendations were endorsed by the Solicitor General of the Ministry of Justice on January 2, 2019. The recommendations laid the foundation for component 1, "*Strengthening the legal and institutional framework*". The core of this component is the development of a data protection legal and regulatory framework to promote trust in the ID system and ensure that personal data being collected under the project is protected. Furthermore, the amendment of the National Identity Management Commission (NIMC) laws are essential to ensure that the Project Development Objectives (PDO) of the Nigeria Identification for Development (ID4D) project is achieved by promoting inclusive and nondiscriminatory processes, protecting personal data, and removing mandatory use requirements and associated criminal penalties of the National Identity Number (NIN).

2. DATA PROTECTION IN NIGERIA

8. The Constitution of the Federal Republic of Nigeria, 1999 (as amended) sets out individual rights of privacy and protections against discrimination. It also delineates the powers that may be exercised by federal, state, and local government.

9. Beyond provisions included in the Constitution and a few sector or agency specific statutes, there is currently no generally applicable comprehensive legal and regulatory framework that protects personal data or individual privacy rights. In addition, Nigeria does not have an institutional or governance body that is mandated to protect the personal data and privacy of citizens. The Data Protection Bill, 2018, which has had several iterations going back to 2014 (namely, the Personal Information and Data Protection Bill 2014, the Data Protection Bill 2015, and the Protection of Personal Information Bill 2016) was passed by the 8th National Assembly on May 16, 2019 and transmitted to the President of the Republic of Nigeria for assent. However, the Data Protection Bill was not assented to and the drafting and enactment process needs to be restarted.

10. Given that the National ID System involves collection, control and processing of personal data, including sensitive data, the absence of an existing robust data protection legislation poses significant legal and reputational risks to the National ID System. This needs to be rectified by putting in place a definitive data protection legislation. The capturing of sensitive data in by the National ID System implicates the twin issues of privacy rights and data protection. A sufficiently robust and well-defined privacy and data protection regime is critical for fostering a trust environment which gives comfort to individuals whose data is captured that their privacy will be respected, and their data will be well protected. A related aspect of this work includes consequential review (and possible revision) to companion cybersecurity and cybercrime provisions.

The key findings of the above mentioned legal and regulatory assessment were:

(a) the present state of privacy and data protection in Nigeria is significantly lacking. The National Information Technology Development Agency (NITDA) regulations are not sufficient to provide protection. There is an urgent need to enact a comprehensive generally applicable data protection legislation consistent with internationally established privacy and data protection principles.

(b) the current cybersecurity legislation needs to be significantly amended to address issues relating to cybersecurity so as to afford the necessary and adequate coverage to Nigeria's National ID System.

(c) a legal and regulatory framework in respect of e-commerce transactions and digital signatures needs to be enacted to create the necessary conditions for the development of National ID in Nigeria.

(d) legislative amendments and/or enactments need to be made to the National Identity Management Commission and National Population Commission legislations to achieve an adequate and enforceable legal and regulatory framework in respect of Nigeria's National ID framework, particularly to ensure that the ID scheme operates in an inclusive, nondiscriminatory and transparent manner.

3. OBJECTIVES OF THE ASSIGNMENT

11. The Government of Nigeria seeks to hire the services of a consulting firm or a consortium of firms to provide legal advice to the Federal Ministry of Communications and Digital Economy (FMCDE) in order to help develop and implement the legal framework, institutional and regulatory capacity for data protection, cybersecurity and ID systems which gives effect to the reforms contemplated by the Project. The overarching objective is to foster an environment of trust around the control and processing of personal data, and the implementation of the ID system, in Nigeria. The objectives of the consultancy assignment are to:

a) draft a comprehensive data protection legislation;
b) draft subsidiary legislations (regulations, rules and/or guidelines) to support the operationalization of primary legislation. This activity will only be carried out after the successful completion of the principal legislation.
c) to draft amendments to existing laws and regulations, including the National Identity Management Commission, National Population Commission legislations, Cybercrimes (Prohibition, Prevention, etc) legislation to harmonize the overall approach to data protection, cybersecurity and cybercrimes in Nigeria and ensure the ID system operates in an inclusive, nondiscriminatory, and transparent manner.

4. SCOPE OF SERVICES

12. The Consultant will conduct and provide an analysis of the Nigeria legal ecosystem including any international obligations, governance frameworks, and stakeholder capacity as

it pertains to data privacy. Based on this assessment, consultant will draft high quality draft legislation and regulations reflecting international good practices such as the European Union General Data Protection Regulations (EU GDPR) which is appropriate for the Nigeria local context.

13. The consultant will consult with the legal working group and be guided by the FMCDE. The consultancy services have been divided into two phases. The first phase is for drafting legislation and the second phase is for drafting regulations. The consultant will undertake a series of consultations with public and private sector stakeholders including the National Assembly.

The Consultant will be required, without limitation, to:

Phase 1: Legislation:

a) Conduct a legal review: The review, without limitation, will include the Constitution of the Federal Republic of Nigeria 1999 (as amended) ("the **Constitution**"), African Charter on Human and People's Rights (Ratification and Enforcement) Act 1983; Armed Forces Act 1994; Births, Deaths, etc., (Compulsory Registration) Act 1992; NIMC Act and Regulations; Cybercrimes (Prohibition, Prevention, ETC) Act 2015; Economic and Financial Crimes Commission Act 2002; Federal Inland Revenue Service (Establishment) Act 2007; Federal Road Safety Commission (Establishment) Act 2007; Corrupt Practices and Other Related Offences Act 2000; Land Use Act 1978; Nigerian Communications Act 2002; National Health Insurance Scheme Act 1999; National Information Technology Development Agency Act 2007; National Population Commission Act 1988; National Youth Service Corps Act 1993; Prisons Act 1972; and Police Act 1943. The review will provide guidance and direction on the drafting of the proposed draft legislation. The review will also assess the current legal instruments and processes, potential risks, possible reforms, and risk mitigation measures necessary for the implementation of the digital identity ecosystem project;

b) Conduct a review to ascertain international best practices such as the EU GDPR. The review will include guidelines, directives, and regulations from international multi-lateral institutions; data protection laws from international and regional bodies, including GDPR and Convention 108+; and lessons learnt from jurisdictions with an established history of data protection administration. The purpose of the review will be to recommend options from various types of legislation and implementation arrangements that may be suited to Nigeria.

c) Conduct stakeholder sensitization, validation and dissemination workshops. These workshops, which shall be held at various stages in the process, will offer the consultants an opportunity to interact with both public and private sector stakeholders for the purposes of gathering the necessary data, raising awareness about the need for a comprehensive data protection regime and validate the findings and obtain feedback from participants in order to finalise the draft legislation.

d) Draft Data Protection legislation. The consultant shall propose piece(s) of legislation to meet Nigeria's objectives to protect personal data and privacy. The proposed draft

legislation shall be submitted to the Official Drafting Personnel of the Federal Ministry of Justice, Abuja upon completion of drafting.

e) Propose amendments to The NIMC Act and the Registration of Persons and Contents of the National Identity Database Regulations 2017 to narrow NIMC's authority to share Personal Data, to specify the third parties who are permitted to receive Personal Data, to prescribe obligations on third parties who receive Personal Data, and to eliminate NIMC's authority to disclose data "for the prevention or detection of crime"; and related implementing regulations have been duly adopted and issued remove the provision that all information contained in the National Identity Database is the property of the Federal Government of Nigeria; and related implementing regulations have been duly adopted and issued.

f) Final Legislation Report. The final report will detail major decisions made during the study, lessons learnt for subsequent legal consultancy studies and recommendations needed for Government to implement the proposed legislation. The recommendations will include processes to establish a data protection commission including timelines, budgets, staffing, administrative procedures, awareness raising and community engagement, etc. The proposed legislation incorporating feedback by the Task Force and participants to the validation workshop will be appended to the report. This report will also propose strategies to ensure buy-in of all relevant stakeholders in the enforcement of national legislation on data protection and privacy.

g) Any other matter(s) incidental to the above and as may be determined by the Project Steering Committee.

h) Phase 2: Regulations

Phase 2 will include all the stages set out above adjusted, wherever necessary, to meet requirements for drafting regulations.

5. DELIVERABLES

14. The Consultant will report to the Coordinator of the Ecosystem Coordination Strategic Unit (ECSU) Abuja. Reports shall be submitted in the official Standard English Language. The reports shall be submitted in Microsoft Word and in line with the schedule stated below.

15. The ECSU requires the deliverables under Phase 1 to be completed within a maximum period of six (6) months and deliverables for Phase 2 will be completed within a period of two (2) months. The definition for the following deliverables is as set out in paragraph 5 above. The deliverables expected of the consultants are as follows:

5.1 Expected Deliverables and Timelines for Phase 1

	Deliverable	Time Frame (from contract signing)	Milestone (%)payment
A1	Inception Report including work plan and timelines	2 weeks	10%
A2	Legal Review Report	2 months	15%
A3	Stakeholder Sensitization Workshops	3 months	0%
A4	Draft Data Protection Bill	6 months	25%
A5	Bill Validation Workshops	7 months	0%
A7	Final Draft Legislation Report	8 months	25%
A6	Capacity Building Workshops	8-10 months	0%

5.2 Expected Deliverables and Timelines for Phase 2

Phase 2 may only be triggered by particular instructions from the Client. The timeframe, measured from contract signing, will therefore depend on the timing of the instructions. The timelines below are for indicative purposes only and are subject to change for the reason advanced above.

	Deliverable	Time Frame (from acceptance of final legislation report)	Milestone payment (%)
B1	Inception Report including updated work plan and timelines (if required)	2 weeks	5%
B2	Legal Review Report (if required)	1 month	
B3	Stakeholder Sensitization Workshops	2 months	0%
B4	Draft Regulations and/or Guidelines	4 months	10%
B5	Regulations Validation Workshops	6 months	0%
B7	Final Regulations Report	8 months	15%
B6	Capacity Building Workshops	8-10 months	0%

6. TEAM COMPOSITION

16. The Consultant shall be a firm or consortium of firms (subcontracting other individuals and firms as needed) whose personnel include legal, regulatory, and technical specialists of high international repute with relevant international experience in their respective areas of expertise. The Consultant will have a thorough understanding of digital identification, data protection, cybersecurity and cybercrime matters, as well as experience advising on law reform processes, drafting legislation, establishing regulatory institutions and advising on data protection matters, with demonstrable knowledge and experience in the areas of work described in these ToRs (particularly, data protection and cybersecurity). The Consultant shall have at least 15 years of demonstrable experience of providing relevant advice in highly developed, complex legal and sectoral contexts. Relevant developing country experience will be an advantage. The selected firm(s) shall provide experts with the following qualifications and experience:

(a) **The Team Leader** shall possess at minimum of a Bachelor's Degree in Law. He or she shall have a minimum of 15 years of relevant experience in the legal profession, including data protection, cybersecurity, cybercrimes, law reform and other matters relating to the establishment, operation and governance of data protection authorities and similar institutions. Experience advising on GDPR compliance is essential. Experience in developing countries as well as demonstrable experience related to the EU GDPR would be an advantage.

(b) **International legal expert(s)** shall possess a minimum of a Bachelor's Degree in Law with at least 7 years of experience in the legal profession in the area of data protection and privacy. Specific experience advising on law reforms, public consultation processes, drafting data protection legislation or regulations, and advising data processers, data controllers and/or data protection authorities is essential. Experience in developing nations as well as demonstrable experience related to the EU GDPR would be an advantage.

(c) **International technology expert** shall possess at a minimum a Bachelor's Degree in Information Technology, Telecommunications, Engineering, Computer Science or related field. The Technology Expert shall demonstrate at least 7 years of experience providing technical solutions or advice on data protection and cybersecurity technologies to data protection agencies, law enforcement and/or private sector data processers and controllers. Specific experience with GDPR compliance would be an advantage.

(d) **Locally qualified legal expert** shall possess a minimum of a Bachelor's Degree in Law and shall be admitted to practice law in Nigeria. He or she shall demonstrate at least 12 years of experience advising on Constitutional and administrative law, judicial review, legal reform and Parliamentary procedure in Nigeria, including drafting primary and secondary legislation. Knowledge of the acceptable practices, norms and standards in drafting primary and subordinate legislation and rules in Nigeria is essential. Experience

advising on the exercise of exclusive, concurrent and residuals powers under the Constitution would be an advantage.

In cases where consortiums are formed, the lead consultant may not submit more than one application. However, the sub-consultant may associate with more than one lead consultant as long as the sub-consultant is not a lead consultant in any of the submissions.

7. SELECTION METHOD

17. The consultant shall be selected in accordance with the **Quality and Cost Based Selection** (QCBS) procedures as set out in the World Bank (WB) Procurement Guidelines.

8. CLIENT'S RESPONSIBILITIES

18. The Client shall have responsibility for providing necessary support to the consultant by:

a) Providing the Consultant with a list of relevant stakeholders.
b) Preparing/extending invitations and follow up with stakeholders for participating in meetings, etc. where necessary.
c) Coordinating and providing location/venue for meetings if necessary.
d) Follow up with stakeholders on collecting information before during and after meetings.
e) Review reports submitted and give feedback within two (2) weeks of report submission.

9. CONSULTANT'S RESPONSIBILITIES

19. All information, data and information obtained from the client shall be properly reviewed and analyzed by the consultant. All such information, data and reports shall be treated as confidential. The Consultant shall make their own arrangements for venue, document reproduction, printing and reproduction of all reports during the assignment.

10. ESTIMATED EFFORT LEVEL AND DURATION OF THE ASSIGNMENT

20. The duration of the assignment shall not exceed six months.

11. PAYMENT SCHEDULE

21. The payment is scheduled as follows:

S/No	Reports	Payment (%)
1	Inception Report including work plan and timelines	10%
2	Legal Review Report	15%
3	First draft Data Protection Bill	25%
4	Final draft Bill report and final legal review reports	25%
5	Regulations, rules and guidelines	25%