NATIONAL INFORMATION TECHNOLOGY AUTHORITY, UGANDA (NITA-U)

UGANDA DIGITAL ACCELERATION PROJECT (UDAP -GOVNET)

TERMS OF REFERENCE FOR PROCUREMENT OF CONSULTANCY SERVICES FOR DEVELOPMENT OF A DATA PROTECTION AND PRIVACY AUDIT AND INSPECTION MANUAL AND CONDUCT OF FIFTEEN (15) PILOT AUDITS WITH THE MANUAL

FEBRUARY 2024

1. INTRODUCTION

Project overview

The Government of Uganda (GoU) represented by the National Information Technology Authority, Uganda (NITA-U/Client) has received financing of United States Dollars Two Hundred Million Dollars (USD 200 million) from the World Bank/IDA toward the cost of the Uganda Digital Acceleration Project – Government Network (UDAP-GovNet) project ID NO. P171305, and it intends to apply part of the proceeds to payments for goods, works, non-consultancy services and consultancy services to be procured under this project. The project includes the following components:

Component 1: Expanding digital connectivity in selected areas
Component 2: Enabling digital transformation of the Government
Component 3: Promoting digital inclusion of host communities and refugees
Component 4: Project Management

Procurement of contracts financed by the World Bank under these components will be conducted through the procedures as specified in the World Bank's Procurement Regulations for IPF Borrowers July 2016 revised September 2023 and is open to all eligible firms and individuals as defined in the procurement regulations. NITA-U shall arrange the publication on its external website of the agreed initial procurement plan and all subsequent updates once it has provided a no objection.

Uganda's context

The Data Protection and Privacy Act was enacted in Uganda in 2019 to give effect to Article 27 of the Constitution, which guarantees the right to privacy. In 2021, the supporting regulations were enacted, which operationalized the Personal Data Protection Office (PDPO) as an independent office under the National Information Technology Authority, Uganda (NITA-U) responsible for implementing and enforcing the law.

Regulation 4 (e) of the Data Protection and Privacy Regulations, 2021 empowers PDPO to conduct audits to ensure compliance by data controllers, processors, and collectors with the Act and these regulations. The PDPO, in fulfilling this mandate intends to engage a consultancy firm, with assistance from the World Bank, to develop a data protection and privacy audit and inspection manual and conduct of fifteen (15) pilot audits with the manual.

2. OBJECTIVE AND SCOPE OF ASSIGNMENT

The consultancy firm shall be required to consult with various players/stakeholders within sectors identified by PDPO and conduct extensive reviews of international, regional, and Uganda's existing data protection and privacy policies, strategies, frameworks, laws, regulations and guidelines on information systems/information security/data protection and privacy audit aimed at informing the development of a data protection and privacy audit and inspection manual and provide comprehensive training to the PDPO staff on how to use the manual.

This will enable the PDPO staff to carry out its statutory mandate through conducting audits and inspection to ensure compliance by data controllers, processors, and collectors with the Data Protection and Privacy Act and supporting regulations as a reference manual. Additionally, the consultancy firm will conduct fifteen (15) pilot audits suing the manual. The Assignment shall involve the following: -

i. Reviewing of literature including but not limited to policies, strategies, frameworks, laws, standards, regulations and best practices to inform the development of a data protection and privacy audit and inspection manual.

ii. Conducting stakeholder consultations within sectors identified by PDPO including the key sectors to be supported under the UDAP-GovNet Program. For the avoidance of doubt, the consultancy firm shall be responsible for managing all workshops and/ or meetings; organize all logistical requirements including but not limited to procuring the venue, food and beverages, public address systems, stationery, rapporteur and sending out invitations for the successful hosting of the stakeholder workshops and/or meeting.

iii. Conducting best practice studies from at least three (3) jurisdictions (***one of which must be from a developing country***) which are advanced in regulation of data protection and privacy and related matters and prepare a best practices report. The consultancy firm shall avail to the Client all documents used to conduct the studies.

iv. Preparing the draft data protection and privacy audit and inspection manual.

v. Conducting a stakeholders' validation workshop to present the data protection and privacy audit and inspection manual for validation. The consultancy firm's role will be to manage the workshop, present the manual and record the deliberations and produce the rapporteur's report. In addition, the consultancy firm shall organize all logistical requirements for the workshop including but not limited to procuring the venue, food and beverages, public address systems, stationery, rapporteur and sending out invitations.

vi. Preparing the final data protection and privacy audit and inspection manual.

vii. Building capacity and training PDPO staff on how to effectively monitor, and assess the compliance of data controllers, collectors and processors with the Data Protection and Privacy Act and supporting regulations using the developed manual.

viii. Conducting of audits fifteen (15) pilot organisations as will be determined by the PDPO at commencement of the Assignment.

ix. Launch of the final data protection and privacy audit and inspection manual.

3. KEY DELIVERABLES AND REPORTING

The expected deliverables for this Assignment are detailed herein below. The deliverables/outputs reports shall be submitted in hard and electronic copies (2 copies each). The consultancy firm shall be required to submit electronic reports in MS Word, pdf files (secured) and presentations in MS Power Point. Reports will be submitted in **English** only.

3.1 TASK 1: KICK-OFF MEETING – OBJECTIVE OF THE ASSIGNMENT AND INFORMATION GATHERING

The consultancy firm shall meet with the PDPO to discuss the Assignment, i.e. the need for and the benefits of developing a data protection and privacy audit and inspection manual for use in monitoring and assessing compliance of data controllers, processors, and collectors with the Data Protection and Privacy Act and supporting regulations, task completion schedule, work plan, approach for performing the Terms of Reference (ToRs) and any other related issues.

The kick off meeting will also be an opportunity for the Client to communicate and/or clarify the outcomes expected from development and use of the manual to conduct fifteen (15) pilot audits.

The consultancy firm shall request in writing and the PDPO shall where the documentation/information is available to them, share information, documents, and other relevant materials that provide background data and information to facilitate the Consultancy. The consultancy firm shall review all provided materials, conduct research on good practices, and develop preliminary questions, areas for further discussion and a list of suggested organizations and stakeholders for in-country meetings.

Task 1 deliverable

Inception report containing a brief of the consultancy firm's understanding of the Assignment, the methodology to be applied by the consultancy firm in conducting the Assignment and a catalogue of information required to perform the Assignment.

3.2 TASK 2: LITERATURE REVIEW TO INFORM DEVELOPMENT OF AUDIT AND INSPECTION MANUAL

The consultancy firm will conduct an extensive literature review on data protection and privacy audit and inspection practices globally. The review will analyze international best practices, standards, and methodologies used in various jurisdictions. The literature review should be comprehensive, covering but not limited to:

a) The existing policies, regulations, and guidelines in the field of data protection and privacy audits and inspections.
b) Innovative methods and tools used in conducting data protection and privacy audits and inspections.
c) Case studies of successful data protection and privacy audit systems from different jurisdictions.
d) Lessons learned and common challenges encountered in conducting data protection and privacy audits and inspections.

The firm shall at its cost conduct research for purposes of identifying the documents that shall be reviewed. The consultancy firm shall convene a meeting with the PDPO to agree on which documents shall be reviewed. The documents include but are not limited to the following: -

a) The Data Protection and Privacy Act, 2019 and supporting regulations
b) Personal Data Protection Office's Strategic Plan

c) ISO/IEC 27701:2019. Privacy Information Management System
d) Information Commissioner's Office UK, Audit Manual
e) Privacy Maturity Assessment Frameworks of countries such as New Zealand, Canada and France among others.
f) Information Technology Audit Framework (ITAF)
g) National Institute of Standards and Technology (NIST) Privacy Framework
h) Center for Internet Security (CIS) Critical Security Controls
i) any other document as may be determined by the Client.

Upon completion of the review, the consultancy firm shall prepare a report and convene a meeting with the PDPO and other key stakeholders to analyze the findings of the literature review to obtain any additional input or concerns. The consultancy firm shall identify the potential policy, legal and regulatory barriers to successful project implementation and measures to address them.

Task 2 deliverable

A literature review report detailing all of the findings, analyses and conclusions from Task 2.

3.3 TASK 3: STAKEHOLDER CONSULTATIONS

The consultancy firm shall prepare a stakeholder consultation plan and conduct stakeholder consultations through face-to-face or virtual discussions and collect all stakeholder comments and prepare a comprehensive summary of key points, challenges, and action items regarding conducting the Assignment. These organizations and stakeholders may include but are not limited to: -

i. Ministry for Information and Communications Technology and National Guidance
ii. National Information Technology Authority, Uganda (NITA-U)
iii. Office of the Director of Public Prosecutions
iv. Uganda Police Force
v. Office of the Auditor General
vi. Regulatory bodies (Bank of Uganda, Uganda Communications Commission, Insurance Regulatory Authority, and National Bureau for Non-Governmental Organisations, PPDA among others)
vii. Data Protection Officers from key sectors that collect personal data either on a large scale or their core activities consist of processing of special personal data

The consultancy firm and PDPO shall convene to review the consultancy firm's questions and to further identify participating organizations and stakeholders required for the meetings and coordination of information gathering. The consultancy firm shall prepare a stakeholders' consultation report on stakeholders consulted. The report shall among others, articulate stakeholders' concerns, recommendations, and "buy-in" for developing and disseminating a data protection and privacy audit and inspection manual.

The consultancy firm shall use the stakeholders' consultation report as a guide for all subsequent meetings, where necessary.

Task 3 deliverable

Stakeholders' consultation report detailing the findings, analysis and conclusions from these consultations.

3.4 TASK 4: BEST PRACTICES STUDY OF OTHER COUNTRIES

The consultancy firm shall provide international best practices from three (3) countries (***one of which must be from a developing country***) that are at a mature level in data protection and privacy regulation and related matters. The consultancy firm shall meet with the PDPO prior to conducting the best practices study to agree on which jurisdictions are best suited for purposes of the study. The firm shall present a proposal of at least five (5) countries who have successfully regulated data protection and privacy and provide justification for the choices to inform the decision on which countries to derive best practices from.

Once the countries have been selected, the consultancy firm will be responsible for arranging, at its own expense, benchmarking study visits to each of the three selected countries. The firm will cover all associated costs, including but not limited to, round-trip air travel, accommodation, and any visa-related expenses for their representatives who are partaking in the study.

In developing the report on best practices, the consultancy firm shall consider the broad perspective of data protection and privacy regulation and related areas ranging from legal and technical aspects, administrative and institutional matters, policy, legal and regulatory frameworks in force. In addition to the aforementioned, for each identified best practice or finding, the consultancy firm shall correlate it with

Uganda's objectives and identify data protection and privacy audit and inspection best practices that are contextualized with Uganda's circumstances.

Task 4 deliverable

A benchmarking study report detailing best practices, analyses and recommendations for Uganda. The report shall list the data protection and privacy audit and inspection practices that exist within international best practice and the specific context in Uganda covering all aspects; policy, legal and regulatory matters, technical, administrative, governance and institutional matters as the circumstances require.

3.5 TASK 5: DRAFT DATA PROTECTION AND PRIVACY AUDIT AND INSPECTION MANUAL AND RAPPORTEUR'S REPORT

(i) The consultancy firm will consolidate findings from Tasks 2-4 to prepare an initial draft of the data protection and privacy audit and inspection manual. This manual should at minimum include but not limited to the following:

a) General purpose and objectives for data protection and privacy audits and inspections.
b) Major elements of data protection and privacy audits and inspections.
c) Description of the data protection and privacy audit and inspection methodology.
d) Reporting and follow-up guidelines.
e) Recommendations documentation.

(ii) The consultancy firm, in collaboration with the PDPO, will then organize a validation workshop, during which the draft manual will be presented to selected stakeholders for their input and suggestions for improvements.

Task 5 deliverable

(i) Draft data protection and privacy audit and inspection manual together with a rapporteur's report following the validation workshop. A comprehensive draft data protection and privacy audit and inspection manual addressing all key aspects of privacy audits and inspections, including templates for use during audits and inspections and the different assessment techniques.

(ii) A detailed rapporteur's report outlining the discussions, feedback, and suggestions from the validation workshop.

3.6 TASK 6: FINAL DATA PROTECTION AND PRIVACY AUDIT AND INSPECTION MANUAL

The consultancy firm shall prepare a substantive, comprehensive and satisfactory data protection and privacy audit and inspection manual in accordance with the objective of the Assignment and Terms of Reference. This will be accompanied with a final report which shall be organized according to the above tasks, and shall include all deliverables and documents that have been submitted to the PDPO. The final report shall include an executive summary discussing the Assignment, the key findings of the literature review, stakeholder consultations, best practices study, validation workshop, final data protection and privacy audit and inspection manual detailing the findings, analyses and conclusions from Tasks 1-5. The consultancy firm shall submit copies of the report in hard and electronic form (2 copies each).

Task 6 deliverable

(i) A substantive and comprehensive final data protection and privacy audit and inspection manual.

(ii) A holistic final report that chronicles the process of manual development, encapsulating key findings, analysis, and conclusions drawn from Tasks 1-5.

3.7 TASK 7: CAPACITY BUILDING AND TRAINING FOR PDPO STAFF

The consultancy firm will undertake a comprehensive training program to ensure PDPO staff understand and can effectively implement the audit and inspection manual. This program should focus on familiarization with the manual, training on the latest best practices in data protection and privacy, enhancing PDPO staff's audit and inspection capabilities, and addressing any challenges in enforcing the Data Protection and Privacy Act and supporting regulations.

The capacity building and training program should include, but not be limited to:

(i) Familiarization with the developed audit and inspection manual, focusing on its application in various scenarios.

(ii) Training on the latest best practices related to data protection and privacy audit and inspection.

(iii) Enhancing the capacity of the PDPO staff to perform comprehensive audits and inspections of data controllers and processors, in order to ensure their adherence to the Act and supporting regulations.

(iv) Addressing any specific areas of concern or challenges faced by the PDPO staff in implementing and enforcing the Data Protection and Privacy Act and supporting regulations.

The consultancy firm shall develop a tailored capacity building and training plan, taking into consideration the current knowledge and skill levels of the PDPO staff, their roles and responsibilities, and the specific requirements of the audit and inspection manual being developed. The training plan should outline the training objectives, modules or topics to be covered, methodology, duration, and evaluation methods.

Task 7 deliverable

Upon completion of the capacity building and training program, the consultancy firm shall provide a comprehensive report detailing the outcomes and recommendations for any further training or capacity building initiatives, if necessary.

3.8 TASK 8: CONDUCTING PILOT AUDITS AND ASSESSING EFFECTIVENESS OF THE MANUAL

The consultancy firm will apply the manual in real-world scenarios by conducting fifteen (15) pilot audits at organisations as will be determined by the PDPO at commencement of the Assignment. These audits will provide crucial feedback on the practical applicability of the manual and highlight areas needing refinement.

Task 8 Deliverables:

(i) Detailed audit plans for each of the fifteen (15) pilot audits.

(ii) Execution of the audits, documented in individual audit reports.

(iii) An encompassing report on findings, reflections, and suggestions for improvements to the manual based on the audit experiences.

3.9 TASK 9: OFFICIAL LAUNCH OF THE AUDIT AND INSPECTION MANUAL

The consultancy firm will collaborate with the PDPO to plan and conduct a formal launch of the finalized data protection and privacy audit and inspection manual, marking its readiness for widespread use.

Task 9 Deliverables:

(i) A launch plan detailing the venue, guest list, media involvement, and launch program.

(ii) Successful execution of the manual launch event, evidenced by media coverage and participant feedback.

(iii) A post-event report documenting the event proceedings, media coverage, and feedback from attendees.

4. EXPERIENCE OF THE FIRM AND QUALIFICATIONS OF THE FIRM

4.1 Experience of the Firm

The Assignment shall be conducted by a consultancy firm.

The firm shall:

(a) At least five (5) years of demonstratable experience and expertise in development of manuals, strategies, policies, reference guides and execution of audits (either ICT, data protection and privacy or compliance audits). It will be an added advantage where such experience is in Government or not for profit sector.

(b) The consultancy firm shall possess expertise in Information Systems Audit, Information Security Assessment or Data Protection and Privacy.

(c) The consultancy firm shall detail the expertise, experience, tasks and how the Assignment will be performed in the technical proposal.

In cases where the firm is not of Uganda origin, it is encouraged to partner with Ugandan experts.

4.2 Expertise and qualifications of the team members

The firm is expected to field a team of key experts and non- key experts including the following key experts who shall collectively have experience in national or regional data protection and privacy frameworks preferably in a developing country, Information Security, policy formulation and stakeholder consultations.

4.2.1 Information Technology/Information Systems Audit Expert

4.2.1.1 Experience

An Information Systems Auditor with professional qualification Information Systems Audit as a Certified Information Systems Auditor (CISA), with at least five (5) years' experience in Information Technology/Information Systems audit, additionally preferably possession of skills in training and capacity building with excellent analytical and reporting skills.

4.2.1.2 Qualifications

a) Bachelor's degree in ICT related field (Computer Science, Information Technology, Computer Engineering, Information Systems, Telecommunication Engineering, Electrical Engineering)
b) Certification in Information Systems Audit (Certified Information Systems Auditor – CISA) is a must,
c) A certification in data protection and privacy or Information Security is an added advantage,
d) Master's degree in an ICT Related Field or MBA is added advantage

4.2.2 Legal advisor in data protection and privacy

4.2.2.1 Experience

A legal advisor with at least five (5) years proven experience in providing advice in areas within the Information and Communications Technology sector or demonstratable experience in data protection and privacy.

4.2.2.2 Qualifications

a) Bachelors of Laws Degree (LLB) is a requirement
b) A certification in data protection and privacy or Information Security is an added advantage,
c) Masters' Degree in Information Technology Law or related field is an added advantage

4.2.3 Information Security Expert

4.2.3.1 Experience

An Information Security expert with five (5) years demonstrable experience in Information Security and a good understanding of the different areas of data protection and privacy.

4.2.3.2 Qualifications

a) Bachelor's Degree in Information Security/Computer Science/Information Technology/Engineering or a related field is a requirement.
b) A certification in risk management or Information Security is a requirement.

5. DURATION OF ASSIGNMENT AND IMPLEMENTATION

The Assignment will be undertaken over a period of **twenty-four (24)** months with **six (6)** months dedicated to the activities of drafting the manual and training users, and **eighteen (18)** months for execution of the **fifteen (15)** pilot audits. The tentative timeframe for implementation of the Assignment is represented as follows:

Time Frame for Implementation of the Assignment

No.	Deliverable	Duration (weeks)	Cumulative (weeks)
1.	Inception report and detailed project plan	2	2
2.	Literature review report	4	6
3.	Stakeholders' consultation report	4	10
4.	Benchmarking study report	4	14
5.	Draft data protection and privacy audit and inspection manual	4	18
6.	Conduct of validation workshop and submission of rapporteur's report	2	20
7.	Final data protection and privacy manual together with report on the Assignment	2	22
8.	Capacity building report	2	24
9.	Fifteen (15) individual audit reports in batches of five. 10% will be paid for each completed batch. An encompassing report on findings, reflections, and suggestions for improvements to the manual based on the audit experiences.	46	70
10.	Post-event report documenting the event proceedings, media coverage, and feedback from attendees.	2	72

The above stated durations are to be understood as guidance and it is the responsibility of the consultancy firm to establish a detailed work plan/schedule within the above time estimates. The estimated staff time inputs should be provided in accordance with the consultancy firm's professional judgment and knowledge of the local conditions and needs. The consultancy firm's work plan/schedule should clearly reflect staff to be deployed and their qualifications and skills for execution of the assignment.

6. SUPERVISION AND ADMINISTRATIVE ARRANGEMENTS

6.1 Supervision

The direct supervision of the Assignment will be done by the National Personal Data Protection Director, **PDPO at the following address:**

Personal Data Protection Office (PDPO)

National Information Technology Authority, Uganda (NITA-U)

Palm Courts, Plot 7A Rotary Avenue (former Lugogo Bypass)

P.O. Box 33151 Kampala, Uganda

6.2 Client's obligations regarding reporting

The Client will provide comments on each report within two (2) weeks of submission, and the consultancy firm will only proceed thereafter.

7. DATA, SERVICES AND FACILITIES TO BE PROVIDED BY THE CLIENT

To the extent possible, the Client will provide free of charge all existing information, data, reports, policies, strategies, laws, regulations in the custody of the Client and will assist the consultancy firm in obtaining other relevant information and materials from Governmental institutions and state authorities as far as possible. Notwithstanding the above assistance, the responsibility to identify the documentation required for the effective execution of the assignment and sourcing of that documentation shall remain with the consultancy firm. The Client will also provide suitable office space to accommodate the consultant's team engaged on the assignment.

The information, data, reports, etc., will be available for the consultancy firm's unlimited use during the performance of the proposed services. For purposes of capacity building and ensuring adequate direct involvement of the client in delivering the final project objectives, the client will assign counterpart staff that shall be agreed upon with the consultancy firm prior to commencement of consultancy services.

8. SERVICES AND FACILITIES TO BE PROVIDED BY THE CONSULTANCY FIRM

In carrying out this Assignment, the consultancy firm shall provide the following services, among others, at its own cost which should be duly provided for in the consultancy firm's proposal:

(a) All costs related to benchmarking visit activities

(b) Office supplies, as required for the period of services;

(c) Utility services and costs;

(d) Accommodation for the consultancy firm's staff while in Uganda;

(e) Subsistence (or per diem) payments for official travel for consultancy firm's staff;

(f) Secretarial and administrative support staff;

(g) International and local telephone services for official communication;

(h) Transport services for official work for the consultancy firm's staff during the term of the Assignment.

9. PAYMENT SCHEDULE

No.	Description	Percentage
1.	Inception report and detailed project plan	20%
2.	Literature review report	20%
	Stakeholders' consultation report	
	Benchmarking study report	
3.	Draft data protection and privacy audit and inspection manual	15%
	Conduct of validation workshop and submission of rapporteur's report	
4.	Final data protection and privacy manual together with report on the Assignment	10%
	Capacity building report	
5.	Fifteen (15) individual audit reports in batches of five. 10% will be paid for each completed batch. An encompassing report on findings, reflections, and suggestions for improvements to the manual based on the audit experiences.	30%
6.	Post-event report documenting the event proceedings, media coverage, and feedback from attendees.	5%