Personal DATA Protection OFFICE

Ref: PDPO/CI/003-CR

26th June, 2025

The Convener,

Digital Agenda Forum,

Munyonyo, Kampala.

CONCERNS REGARDING THE MASS NATIONAL ID RENEWAL AND PROTECTION OF PERSONAL DATA IN UGANDA

The Personal Data Protection Office (PDPO) acknowledges receipt of your open letter dated 16th June 2025 and appreciates your engagement on matters concerning the ongoing mass enrolment and renewal exercise for national identity cards that is being conducted by the National Identification and Registration Authority (NIRA).

PDPO formally sought clarification from NIRA, the data controller for the exercise on some of the concerns highlighted by the Digital Agenda Forum. Following review of submissions contained in NIRA's response dated 24th June 2025 as well as consideration of previous engagements with NIRA and PDPO's ongoing regulatory oversight, we are pleased to address the requests within your open letter as follows;

1. **Clarify why there appears to be an overcollection of personal data and biometric data, including facial, fingerprints, and the iris scans, during the national ID renewal process, and provide the legal justification for collecting this volume and sensitivity of data under the Data Protection and Privacy Act, Cap. 97**

   The determination of the legal basis and necessity for collecting and processing personal data, including biometric data is the responsibility of the data controller. In this context, NIRA acts as the data controller for the mass enrolment and renewal of national identity cards.

   Section 7(2)(b)(i) of the Data Protection and Privacy Act, Cap. 97 provides that personal data may be collected and processed if it is necessary for the proper

performance of a public duty by a public body. Since NIRA is mandated under Section 5 of the Registration and Persons Act, Cap 332, to manage the National Identification Register and issue national identification cards, the collection of personal data, including biometric data falls squarely within the performance of its statutory functions.

Section 12 of the Data Protection and Privacy Act, Cap. 97 requires that personal data must be collected for a specific, lawful, and explicitly defined purpose. In this case, the purpose is to facilitate accurate identification and registration of Ugandan citizens and residents as required by law. Section 14 further stipulates that a data controller must process only personal data that is necessary or relevant for the purpose for which it is collected, emphasizing the principle of data minimisation.

NIRA in their letter dated 24th June 2025, explained that the collection of biometric data (including fingerprints, facial images, and iris scans) is grounded in Regulation 15(1)(c) of the Registration of Persons (Registration) Regulations, SI No. 67 of 2015, which authorises the capture and recording of such data for registration. NIRA also clarified that additional modalities, such as iris scans, are needed to ensure robust identity de-duplication and to enhance accuracy and inclusion, such as those whose fingerprints may not be reliably captured, such as the elderly and persons with disabilities. Additionally, NIRA also referenced international good practice, including guidance from the World Bank's ID4D Initiative and relevant ISO/ICAO standards, in support of its biometric approach. These standards recommend the use of multiple biometric modalities to enhance the resilience and inclusivity of foundational identity systems.

Based on the above, PDPO finds that the collection of biometric data, namely facial images, fingerprints, and iris scans during the mass enrolment and renewal of national IDs is lawful, necessary, and proportionate. It is justified under the above-mentioned applicable laws. PDPO is satisfied that NIRA's collection of this data does not

contravene any of the data protection principles under Section 3 of the Data Protection and Privacy Act, Cap 97.

2. **Confirm whether Data Protection Impact Assessments have been conducted by NIRA and the associated institutions and whether they are publicly available.**

PDPO acknowledges the initial steps taken by NIRA to incorporate data protection and privacy safeguards in the ongoing mass enrolment and renewal of national identity cards. In response to PDPO's guidance dated 4th March 2024, NIRA initiated a structured risk evaluation process that aligns with key principles of a Data Protection Impact Assessment (DPIA), as provided for under Regulation 12 of the Data Protection and Privacy Regulations.

Although a comprehensive DPIA is still in development, PDPO notes that NIRA has implemented several foundational components of the DPIA process in a phased and risk-based manner. These early interventions have already contributed to the following notable improvements:

- With support from PDPO, NIRA conducted a general data protection and privacy training for all its more than 400 permanent staff on 30th March 2024. In addition, between January and May 2025, NIRA, in collaboration with PDPO, held a series of specialized training sessions targeting staff directly involved in the registration and renewal processes;
- A data protection and privacy notice is now displayed to applicants on the NIRA web portal, ensuring individuals are informed about their rights and how their data will be processed;
- Data collected during the renewal process is now limited to what is necessary, as NIRA retains existing core identification data;
- The improved process allows applicants to view their captured data via a display and confirm its accuracy before submission, ensuring that personal information remains current and correct;

- Various updated data protection, privacy, and security policies have been developed, as outlined in NIRA's attached response. This supports compliance with the accountability principle under the Data Protection and Privacy Act.

The comprehensive DPIA process remains ongoing under PDPO oversight and upon completion, NIRA will publish a summary of the DPIA highlighting key risks and mitigation measures, with sensitive information redacted for national security. Additionally, PDPO will review the newly developed policies as part of the planned audit of NIRA in the next financial year.

PDPO finds that NIRA has demonstrated credible progress towards conducting a comprehensive DPIA and is strengthening compliance with data protection principles. The Office will continue to monitor and support NIRA to ensure full alignment with the Data Protection and Privacy Act, Cap. 97.

3. **Clarify whether the current biometric data collection falls within NIRA's mandate under the Registration of Persons Act, Cap. 332.**
   This matter has been substantively addressed under the response to Request 1. For emphasis, PDPO confirms that the collection of biometric data by NIRA is squarely within their statutory mandate. Regulation 15(1)(c) of the Registration of Persons (Registration) Regulations, SI No. 67 of 2015 explicitly authorises the collection and recording of biometric data necessary for registration.

   PDPO is satisfied that the current collection of biometric data by NIRA fully aligns with its legal mandate under the Registration of Persons Act, Cap. 332 and the supporting Regulations.

4. **Confirm whether PDPO has issued or intends to issue any guidance regarding the integration of National Identification Number (NIN) across essential services.**
   PDPO acknowledges the importance of developing regulatory guidance on the

integration of the NIN across essential services. While such guidance has not yet been issued, we recognise the significance of this issue and have prioritised its inclusion in our upcoming regulatory agenda.

5. **Provide assurance that all third-party institutions requiring the national ID, particularly banks and telecom operators are registered with PDPO, have appointed Data Protection Officers, and are compliant with the law.**

   PDPO provides the following assurance regarding compliance among third-party institutions, particularly banks and telecommunications operators that require access to the national identification register for their operations:

   Pursuant to the circular by NIRA dated 1st June 2023, a copy is attached for ease of reference, NIRA instructed the 75 entities that were accessing data through NIRA's third-party interface to register with PDPO. This registration with PDPO also necessitates the appointment of a Data Protection Officer. Below is a brief on the status of the entities' registration status;

   - **Banks and Microfinance Deposit-Taking Institutions (MDIs):** As of 25th June 2025, 96% of the 28 banks and MDIs listed in NIRA's circular are registered with PDPO and have renewed their registration as required by law. Only one entity has an expired registration and has yet to renew. This institution has been formally notified and required to regularise their registration within five days.
   - **Telecommunications and mobile money operators:** Of the eight (8) active providers listed in NIRA's circular, seven (7) are currently registered and have renewed their registration with PDPO. The remaining provider will similarly be issued a formal notice to comply within five days.
   - **Market Exits:** Entities that have exited the Ugandan market, such as Africell, Smile Telecom, EFC Uganda, and Mercantile Credit Bank are excluded from these compliance numbers, as they no longer fall within the regulatory scope.

We further clarify that, contrary to the figure referenced in your open letter, as of 25th June 2025, the total number of registered data controllers and processors with PDPO stands at over 6,300. This number continues to grow as more entities comply with their obligations under the law. Notably, our preliminary assessment indicates that the Digital Agenda Forum collects and/or processes personal data as part of its activities and is therefore required to register with PDPO.

6. **Publicly share any data sharing agreements and security safeguards relating to the current National Identification Number (NIN) collection and usage.**

   On the matter of data sharing, PDPO has provided guidance to NIRA on the required elements of data sharing agreements to ensure compliance with the Data Protection and Privacy Act, Cap. 97 and its Regulations. Additionally, PDPO supported NIRA in developing a compliance checklist for assessing third-party entities before sharing or granting access to personal data. NIRA, as the custodian of the National Identification Register, maintains all such agreements, and requests for specific documents should be addressed directly to NIRA. Regarding security safeguards, PDPO will continue to review and verify their effectiveness, particularly during the forthcoming data protection and privacy audit scheduled for the next financial year.

7. **Outline the steps your Office is taking to ensure that all data processing associated with this exercise is transparent, lawful and subject to enforcement.**

   PDPO is committed to ensuring that all data collection and processing associated with the mass national ID enrolment and renewal exercise is transparent, lawful, and subject to enforcement. In furtherance of this mandate, PDPO;

   - Conducted training for NIRA staff, all of whom signed a data protection and privacy commitment pledging to safeguard confidentiality and integrity, practice data minimisation, facilitate data subject rights, and uphold accountability and transparency in line with the law.
   - Ensured that a clear and accessible data protection and privacy notice is displayed to data subjects on the NIRA pre-registration portal.

Personal
DATA
Protection
OFFICE

- Continues to monitor and support DPIA processes and require public disclosure of a summary (with sensitive data protected); and
- Is finalising an audit and inspection manual and has prioritised NIRA for a comprehensive data protection and privacy audit in the upcoming financial year.

We would like to appreciate the Digital Agenda Forum for raising these important questions and for recognizing the work done by PDPO in safeguarding personal data and privacy. We also acknowledge NIRA's cooperation in providing detailed clarifications and implementing improvements in response to our guidance. PDPO will continue to monitor compliance, finalize the audit and inspection manual, and prioritize a full audit of NIRA in the coming financial year. We remain available for further engagement and encourage continued collaboration to ensure the protection of personal data and safeguarding of privacy throughout the national ID enrolment and renewal process.

Baker Birikujja

AG. NATIONAL PERSONAL DATA PROTECTION DIRECTOR

Copy to: Permanent Secretary, Ministry of ICT and National Guidance
Executive Director, National Identification and Registration Authority (NIRA)
Executive Director, National Information Technology Authority, Uganda (NITA-U)

National Identification and Registration Authority
Uganda- My Country My Identity

Our Ref...

NIRA/ED/ PDPO /19/06/2025

24th June 2025

Ag. National Personal Data Protection Director
National Personal Data Protection Office
Palm Courts
KAMPALA, UGANDA

RE: RESPONSE TO CONCERNS REGARDING THE MASS ENROLMENT AND RENEWAL EXERCISE FOR NATIONAL IDENTITY CARDS

The National Identification and Registration Authority (NIRA) acknowledges receipt of the letter from your office regarding issues raised by the Digital Agenda Forum dated 18th June 2025, expressing concerns regarding the ongoing National Identification Number (NIN) renewal exercise and the associated data protection practices.

Below is NIRA's official response to the specific concerns raised by the Digital Agenda Forum:

Issue 1: The process involves the collection of extensive Biometric data including an individuals full names, date and place of birth, details of origin and tribe, names of parents, a passport style facial photograph, signature, fingerprint, and an iris scan

The National Identification and Registration Authority (NIRA) is established under Section 4 of the *Registration of Persons Act*, Cap 332 (ROPA), and is mandated under Section 5(1)(a) to, among others, create, manage, maintain, and operate the National Identification Register (NIR); to register all citizens of Uganda; and to issue them with National Identification Numbers (NINs) and National Identity Cards.

In executing this mandate, **Regulation 15(1)(c)** of the *Registration of Persons (Registration) Regulations*, S.I. No. 67 of 2015, provides that where the Authority is prima facie satisfied that an applicant for registration has provided all required information, it shall take and record the applicant's fingerprints or other biometric information.
Under **Regulation 2**, "biometric information" is defined to include: *DNA, fingerprint, eye retina, iris, voice pattern, facial pattern, and hand measurements.*

Consistent with these provisions, NIRA currently captures **fingerprints, signature, facial images, and recently, iris**. The inclusion of the **iris** is fully within the legally recognised biometrics scope and aligned with global best practices for biometric systems. This measure

Kololo Independence Grounds, P.O. Box 26529 Kampala, Uganda, Tel: +256-312-119-600
www.nira.go.ug, Email: info@nira.go.ug

is intended to strengthen identity de-duplication, enhance reliability, and future-proof the identity system.
Importantly, the addition of iris capture was a response to challenges faced by certain populations—particularly the **elderly and persons with disabilities**—whose fingerprints may be wor, missing or unreadable. Incorporating the iris as an additional biometric modality enables broader inclusion and improves the accuracy of identity verification.
It is therefore important to underscore that all processes undertaken by NIRA are fully grounded in the law and conducted in compliance with established statutory and regulatory frameworks.

Issue 2: The scale, sensitivity and manner of data being collected under this process, especially given that the National ID is now a mandatory requirement for essential services.

NIRA acknowledges the critical importance of balancing the need for accurate identity management with the rights and expectations of individuals concerning the protection of their personal data. In this regard, NIRA affirms that the scale, sensitivity and manner of data collection under both the initial registration and renewal processes is:

a) Lawful and Necessary

All data collected is strictly within the scope of NIRA's statutory mandate under **Section 5(1)(a-c) of the Registration of Persons Act (ROPA), Cap 332**, which empowers the Authority to register citizens, maintain the National Identification Register, and issue National Identification Numbers (NINs) and ID cards.

Specifically:

- **Biographical data** (e.g., names, date/place of birth, parentage, origin) is required to determine **citizenship eligibility**, especially for persons registering as citizens by birth(descent), in line with **Article 10 of the Constitution**.
- **Biometric data** (fingerprints, facial image, signature, and iris) is necessary for **identity verification and removing duplicates**, ensuring that each individual is registered only once.

b) Collected for a Specific and Lawful Purpose

Data collection is conducted in accordance with the **Purpose Specification and Limitation principles** outlined in the **Data Protection and Privacy Act, 2019**, and is strictly limited to what is required to:

- Establish and confirm identity;
- Ensure accurate population data for government planning and service delivery;
- Prevent identity fraud and duplication.

Under **Section 65(1) of ROPA**, the Register's data may only be used for lawful functions, including:

- National ID and passport issuance,
- Immigration control,

- National security,
- Public service provision (e.g., health, education, social security),
- Revenue administration and law enforcement.

c) Proportionate and Aligned with Best Practices

The biometric modalities used by NIRA are consistent with **international standards for foundational identity systems**, such as those recommended by the **World Bank ID4D Initiative** and **ISO/ICAO guidelines**. The **inclusion of iris capture** enhances inclusivity—particularly for individuals with worn or unreadable fingerprints—and strengthens the overall accuracy and future-resilience of the identity system.

The extent of data collected is **proportionate to its purpose** and is not excessive. NIRA does not collect data for speculative or unrelated uses.

d) Subject to Strict Safeguards

All data collected is stored and processed in compliance with the **Data Protection and Privacy Act**, including the principles of:

- Lawfulness,
- Transparency,
- Data minimization,
- Security and confidentiality.

In addition, access to the data is strictly controlled and limited to authorized personnel and institutions as prescribed under the law.

Issue 3: *Expanding the use of the NIN across Government Services*

The integration of the National Identification Number (NIN) into the delivery of public and private services is the result of a deliberate Government effort to establish a unified, secure, and efficient identity management framework. This effort began with the enactment of the Registration of Persons Act, Cap. 332, and continues through the ongoing implementation of policies and systems that utilize the NIN as a foundational identity credential across sectors.

When Parliament passed the Registration of Persons Act (ROPA), it did so with a clear policy intention to:

- Eliminate duplication in laws and processes governing identity registration;
- Harmonise disparate identity databases across Government and the private sector;
- Establish a central registration authority (NIRA) with a mandate to maintain the National Identification Register; and
- Provide for regulated access and use of identity data by authorised Government institutions and service providers.

This is explicitly captured in Section 2 of the Act, which defines the purpose as:

"(a) to remove duplication from the processes and laws relating to registration of persons; (b) to harmonise and consolidate the law on registration of persons; (c) to establish a central registration body for the registration of all persons in Uganda; (d) to establish a national

identification register of all persons in Uganda; and (e) to provide for access and use of the information contained in the national identification register."

Section 65 of ROPA outlines the lawful purposes for which data in the National Identification Register may be accessed and used. These include:

- Issuing National and Alien ID Cards
- Passport issuance, immigration and border control
- National security and law enforcement
- Statistical and administrative purposes
- Taxation, anti-money laundering, and anti-human trafficking
- Delivery of health, education, and social protection services
- Any other lawful purpose as may be determined by the Minister

Additionally, Section 65(3) authorises Ministries, Departments, and Agencies (MDAs) to access and use data in the register for these purposes, making NIRA's identity framework a central pillar in modern governance.

In line with the above, Section 66 of the Act mandates all MDAs and institutions providing public services to require the NIN or National ID from individuals seeking to access services such as:

- Employment
- Voting and passport application
- Opening of bank accounts and obtaining credit
- Land registration and property transactions
- Pension and social security services
- Insurance, taxation, and financial transactions
- SIM card registration and other ICT-based services

These provisions reflect the Government's legislative decision to adopt a single, reliable identifier for use across the public and private sectors—anchored in law and administered by NIRA.

The use of the NIN across platforms such as the Tax Identification Number (TIN), e-passport issuance, and SIM card registration is part of the implementation phase of this national policy highlighted in the Registration of Persons Act Cap. 332.

Issue 4:Legal Framework and potential Non compliance

See the table attached and marked as Annex 1

Issue 4: Such systemic integration, while possibly intended for efficiency, increases risks of profiling, surveillance, identity theft, and exclusion if not adequately regulated.

NIRA is fully aware of concerns regarding profiling, surveillance, identity theft, and exclusion as the NIN becomes central to services. Our operations are designed to actively mitigate these risks:

i. **Profiling (Automated analysis of personal data for behavioral prediction):** NIRA's mandate is solely **identity establishment and verification**, not behavioral analysis. Data collection is strictly for unique identification, with "verification-only" services for third parties to prevent profiling.
ii. **Surveillance (Close monitoring, often covert):** NIRA is an identity authority, not a surveillance agency. We do not track individuals. Access to the National Identification Register (NIR) is **highly restricted** (need-to-know, least privilege), legally governed, and meticulously audited, preventing unauthorized monitoring.
iii. **Identity Theft (Using another's identity without permission):** Our primary defense is **robust multi-modal biometrics** (fingerprints, face, iris), which ensures unique identity and strong de-duplication, making impersonation extremely difficult. Data is held in secure, encrypted infrastructure, and legal penalties deter fraud.
iv. **Exclusion (Denial of services due to identity issues):** NIRA's core mission is **universal registration and inclusion**. We actively address barriers through biometric enhancements (e.g., iris scans for the elderly), flexible identity proofing (relative identification), and accessible grievance mechanisms, ensuring every eligible Ugandan can register. This matter was clearly addressed in the recent case of ***Initiative for social and economic Rights (ISER) and Ors vs AG and NIRA Miscellaneous Cause No. 0086 of 2022*** *in which Hon. Justice Boniface Wamala stated it was not true that by its nature and design the Ugandan National ID system is exclusionary and discriminatory*

In essence, while the NIN's utility expands, NIRA's processes are legally compliant, technologically secure, and operationally transparent, firmly dedicated to inclusion, security, and upholding the privacy rights of all Ugandans.

Their Formal Requests

1. In response to the formal requests, it is noted that Requests 1 and 3 have been comprehensively addressed under Issues 1 and 2 respectively.

2. Confirm whether DPIAs have been conducted by NIRA and the associated institutions and whether they are publicly Available

NIRA commenced the process of conducting a Data Protection Impact Assessment (DPIA) for the ongoing Mass Enrolment and Renewal exercise. An initial internal review has been undertaken, and the Authority is currently working—together with the Personal Data Protection Office (PDPO)—to complete a comprehensive DPIA for this national exercise.

This process remains ongoing and demonstrates NIRA's commitment to ensuring that all data collection and processing activities are lawful, necessary, and subject to appropriate risk mitigation.

3. **Publicly share any data sharing agreements and security safeguards relating to the current NIN collection and Usage**

The National Identification and Registration Authority (NIRA), under Sections 65(3) and 67 of the Registration of Persons Act (Cap. 332), is mandated to facilitate lawful access to information in the National Identification Register (NIR). This is done in full compliance with the Data Protection and Privacy Act, 2019.

1. Data Sharing Framework
Access to NIR data by third parties (e.g., banks, telecoms) is governed through formal **Memoranda of Understanding (MoUs)** and **Data Sharing Agreements (DSAs)**. These are only signed with entities that:

i. Are registered with the **Personal Data Protection Office** under Section 29 of the Act;
ii. Demonstrate respect for **data subject rights**, including obtaining consent or court orders where necessary;
iii. Commit to achieving **compliance with international standards** such as ISO/IEC 27001.

2. Verification-Only Access
Most private institutions receive **verification-only services**. They submit a National Identification Number (NIN) for validation and receive only a **"Yes" or "No"** response—no personal data is disclosed. This ensures privacy while enabling regulatory compliance (e.g., KYC).

3. Security and Oversight
Data access is protected through:

i. Role-based and mulitfactor authentication and secure APIs;
ii. Encryption of data in transit and at rest;
iii. Full audit trails and oversight by both NIRA and the PDPO.

Why MoUs Cannot Be Publicly Shared
While NIRA is committed to transparency, **individual MoUs and their addenda are not publicly disclosed** due to:

i. **Confidentiality obligations** with partner institutions;
ii. The **sensitive nature of national identity data**;
iii. The need to prevent the exposure of **technical or operational safeguards** that could compromise system security.

These agreements are, however, subject to **rigorous legal vetting**, **regulatory oversight**, and are executed in accordance with Uganda's data protection framework.

7. Steps taken to ensure the registration and renewal process is transparent as required by the Data Protection and Privacy Act

NIRA is committed to upholding the principles of transparency and accountability in all its registration and renewal activities, as mandated by the Data Protection and Privacy Act. Our approach is multi-faceted, encompassing robust legal frameworks, advanced technical safeguards, dedicated human capital, and proactive public education.

i. Strong Legal and Policy Frameworks

Our commitment to transparency begins with strict adherence to the law:

- **Compliance with National Laws:** All NIRA activities are rigorously governed by the **Data Protection and Privacy Act (Cap 97)** and the **Registration of Persons Act**

(Cap 332). These laws establish explicit parameters for lawful data collection, processing, storage, and sharing, fundamentally anchored in principles of consent, purpose limitation, data minimization, and, crucially, **transparency in data handling**.

- **Comprehensive Internal Policies:** NIRA has developed and mandates adherence to **20 detailed internal data governance policies**. These policies, include:
    - Information Security Policy
    - Acceptable Use Policy
    - Access Control Policy
    - Change Management Policy
    - Clear Desk and Screen Policy
    - Cryptography Key Management Policy
    - Data Breach Response Policy
    - Data Backup and Recovery Policy
    - Database Credentials Policy
    - Data Processing Policy
    - Data Protection and Privacy Policy
    - Digital Forensics Policy
    - Email Management Policy
    - Human Resource Security Policy
    - Mobile Device Policy
    - Password Protection Policy
    - Secure Development Policy
    - Technology Disposal Policy
    - Third-Party Management Policy
    - Incident Management Policy They provide explicit guidance on secure data handling, access controls, and incident response, all contributing to a transparent operational environment.

ii. Advanced Technical and Operational Safeguards

NIRA embeds security and transparency into every stage of the registration process through the measures below. Each safeguard reinforces citizens' trust while upholding the integrity of the National Identification Register (NIR).

i. Informed Consent by Design

Every enrolment begins with a clear, plain-language consent notice. Applicants are told what data is collected, why it is needed, how long it will be kept, and how they can exercise their data-protection rights before any information is captured.

ii. End-to-End Data Encryption

All personal data is encrypted at rest in NIRA's secure data centres and in transit across internal networks and public channels. This cryptographic layer preserves confidentiality and prevents tampering—thereby underpinning transparent, trustworthy processing.

iii. Granular, Role-Based Access Controls

Access to NIR data is allocated strictly on a need-to-know basis. Detailed audit logs record who accessed what, when, and for what purpose, ensuring accountability and enabling rapid investigation of any irregular activity.

iv. Monitored Infrastructure

NIRA's data centres are protected by multilayered defences—firewalls, intrusion-detection systems, endpoint security, and regular cyber-resilience assessments. These controls guard against unauthorised interference and keep operations verifiably secure.

v. Applicant-Facing Enrolment Screens

Every biometric kit now includes a secondary display that mirrors the data being entered. Applicants can review and confirm each field in real time, reducing capture errors and making the process visibly transparent.

vi. Online Pre-Registration Portal

Citizens may initiate enrolment online, providing their details directly and reviewing them before submission. This self-service step gives individuals greater control over their information and shortens in-person processing times.

Together, these safeguards create a robust ecosystem in which data integrity, citizen oversight, and operational transparency reinforce one another—delivering a registration experience that is both secure and accountable.

iii. Human Capital and Institutional Accountability

Our personnel are fundamental to ensuring transparent operations:

i. **Mandatory Staff Training:** All permanent (400+) and temporary staff (10,000+) underwent intensive and ongoing training in data protection, privacy principles, and **ethical data management**, emphasizing their role in transparent and accountable processes together with the Data Protection Office.
ii. **Confidentiality Agreements:** Every employee signs a legally binding confidentiality agreement, reinforcing their obligation to handle data with integrity and transparency. Breaches are subject to strict disciplinary and legal action.
iii. **Dedicated Data Protection Officer (DPO):** NIRA has appointed a dedicated Data Protection Officer, tasked with monitoring compliance, conducting internal audits, and implementing best practices, serving as a key figure in ensuring institutional transparency and accountability.

iv. Public Education on Data Rights

Empowering citizens with knowledge about their data rights is a critical strategy for fostering transparency and trust:

1. **Public Awareness Campaigns:**
    - **Multimedia Outreach:** We actively disseminate simplified information about our activities through various multimedia channels, including national radio, TV, newspapers, and social media platforms, making complex information accessible.
    - **Community Engagement:** In partnership with local leadership, NIRA has established **District Mass Enrolment and Renewal Committees**. These committees, which include representatives such as the RDC (Chairperson), LCV

Chairperson, DPC, Electoral Commission representative, and NIRA staff (Secretary), support mobilization and outreach. This includes securing **free airtime on district radio stations**, ensuring wide public awareness and transparent communication about the exercise and citizen rights.

2. **Accessible and User-Friendly Information:**
    - **Official Website:** NIRA's website serves as a central hub, providing detailed resources on data protection, including our privacy policies, FAQs, and clear channels for raising concerns, all contributing to an open information environment.
3. **Transparent Consent and Notification Mechanisms:**
    - **Informed Consent:** During both registration and renewal, individuals are **clearly informed** about what data is being collected, the specific purpose of collection, and how it will be used. **Explicit consent is sought**, ensuring that data collection is not covert.
    - **Privacy Notices:** In compliance with **Section 13 of the Data Protection and Privacy Act**, all registration platforms now feature a comprehensive **privacy notice**. This notice explicitly informs applicants about NIRA's identity, the lawful basis for data collection, the purposes of processing their data, and their rights—thereby reinforcing accountability and fundamental transparency.

Conclusion

The National ID is a cornerstone of Uganda's digital and administrative infrastructure. NIRA is committed to ensuring that its rollout is conducted in strict compliance with national laws, constitutional guarantees of privacy, and international obligations.

We welcome continued engagement with the Digital Agenda Forum and other civil society stakeholders and reaffirm our readiness to provide additional clarity, participate in dialogue forums, and support the PDPO's regulatory initiatives.

R. Kisembo

Rosemary Kisembo
EXECUTIVE DIRECTOR

Cc: Permanent Secretary, Ministry Of ICT and National Guidance
National Information Technology Authority, Uganda (NITA-U)

A ANNEX 1

S/N	HIGHLIGHTED LEGAL PROVISIONS UNDER DATA PROTECTION AND PRIVACY ACT CAP.97 AND HOW NIRA COMPLIES		
1.	Section 10 – Right to Privacy	Prohibits unlawful or arbitrary collection, processing, or use of personal data.	NIRA operates strictly under the Registration of Persons Act (Cap 332) and the Data Protection and Privacy Act, ensuring all personal data is collected for lawful, specific purposes related to national identity.
2.	Section 12 – Data Minimization	Data collected must be adequate, relevant, and not excessive in relation to its purpose.	NIRA collects only data that is necessary for identity verification and citizenship determination (e.g., name, date of birth, fingerprints, iris). Data minimization is a core principle in NIRA's biometric enrolment policies.
3.	Section 13 – Transparency & Notification	Data subjects must be informed about the purpose, nature, and recipients of the data being collected.	At all registration points, NIRA provides privacy notices, explains the purpose of data collection, and obtains informed consent. Applicants are guided through what is being collected and why.
4.	Section 19 – Cross-Border Data Transfers	Data should not be transferred outside Uganda unless adequate safeguards exist.	NIRA's servers and data centers are located in Uganda, and personal data is not transferred across borders. Any potential sharing must comply with safeguards set by the NITA-U regulations.
5.	Sections 24–33 – Data Subject Rights	Includes rights to access, rectification, erasure, objection, and compensation.	NIRA allows citizens to request corrections of errors, update their information, and access their NIN records through designated procedures. Mechanisms for rectification and redress are embedded in its change of

			particulars and appeal processes.

National Identification and Registration Authority
Uganda- My Country My Identity

Our Ref... **NIRA/ED/ADM/2A/23-231**

01st June 2023

The Distribution List Attached

CERTIFICATE OF REGISTRATION AS DATA COLLECTOR/DATA PROCESSOR/DATA CONTROLLER

The National Identification and Registration Authority (NIRA) is implementing measures to ensure the protection of personal data and requires all entities that access personal data held by NIRA to submit the necessary certifications. The Data Protection and Privacy Act 2021 and Regulations under the Act require a data collector/data processor/data controller to register with the Personal Data Protection Office.

As an entity that accesses personal data held in the National Identification Register through the Third-Party Interface (TPI) of NIRA, I am writing to request you to submit to NIRA a copy of your valid certificate of registration as a registered data collector/data processor/data controller issued by the Personal Data Protection Office.

Should you have any questions or require further clarification regarding this request, please do not hesitate to contact our Manager Legal Advisory Services Ms. Brenda Kezaabu Agaba brenda.kezaabu@nira.go.ug or our Manager Compliance and Enforcement, Mr. Bahemuka John Toa; john.bahemuka@nira.go.ug. We value your commitment to data protection and appreciate your prompt attention to this matter.

Thank you for your cooperation, and we look forward to receiving the required document at your earliest convenience but in any case, not later than 30th June 2023.

Brig *(Rtd).* Stephen Kwiringira
FOR: EXECUTIVE DIRECTOR

Copy: The National Personal Data Protection Director, Personal Data Protection Office

The Distribution List:

1. The Chief Executive Officer, ABC BANK
2. The Chief Executive Officer, ABSA BANK
3. The Chief Executive Officer, AFRICEL
4. The Chief Executive Officer, AIRTEL
5. The Chief Executive Officer, BANK OF AFRICA
6. The Chief Executive Officer, Bank of Baroda
7. The Chief Executive Officer, Bank of India
8. The Chief Executive Officer, Bayport
9. The Chief Executive Officer, BRAC Bank UGANDA
10. The Chief Executive Officer, CAIRO BANK
11. The Chief Executive Officer, Centenary Bank
12. The Director, Directorate of Citizenship and Immigration Control
13. The Managing Director, DFCU BANK
14. The Chief Executive Officer, DTB BANK
15. The Chief Executive Officer, Eco Bank
16. The Chief Executive Officer, EFC
17. The Chief Executive Officer, EQUITY BANK
18. The Chief Executive Officer, EXIM BANK
19. The Chief Executive Officer, Experian CRB
20. The Chief Executive Officer, Fido Credit
21. The Chief Executive Officer, Finance Trust Bank
22. The Chief Executive Officer, FINCA
23. The Chief Executive Officer, Future Link Technologies
24. The Chief Executive Officer, Gnugrid Africa Ltd
25. The Chief Executive Officer, GTB BANK
26. The Chief Executive Officer, HCM Public service
27. The Chief Executive Officer, HOUSING FINANCE BANK
28. The Inspector General of Government, Inspectorate of Government
29. The Chief Executive Officer, IOTEC Limited
30. The Chief Executive Officer, IZZY SERVICESINT LTD
31. The Chief Executive Officer, KCB BANK
32. The Chief Executive Officer, Laboremous
33. The Chief Executive Officer, LYCA MOBILE
34. The Chief Executive Officer, MERCANTILE Bank
35. The Chief Executive Officer, Metropole
36. The Permanent Secretary, Ministry of Agriculture
37. The Permanent Secretary, Ministry of Education

38. The Permanent Secretary, Ministry of Energy
39. The Permanent Secretary, Ministry of Gender Labour and Social Development
40. The Permanent Secretary, Ministry of Lands
41. The Permanent Secretary, Ministry of Public Service
42. The Permanent Secretary, Ministry of Works
43. The Permanent Secretary, Ministry of Health
44. The Chief Executive Officer, MTN
45. The Executive Secretary, National Building Review Board
46. The Chief Executive Officer, NCBA BANK
47. The Executive Director, NITA - U
48. The Managing Director, NSSF
49. The Auditor General, Office of Auditor General
50. The Chief Executive Officer, Opportunity Bank
51. The Chief Executive Officer, ORIENTBANK/I&M Bank
52. The Chief Executive Officer, Pegasus Tech
53. The Executive Director, Petroleum Authority Uganda
54. The Chief Executive Officer, Pivot Payments
55. The Chief Executive Officer, Post Bank
56. The Chief Executive Officer, Pride Microfince Bank
57. The Chief Executive Officer, RIPPLENAMI
58. The Chief Executive Officer, SMILE Telecom
59. The Chief Executive Officer, Stanbic Bank
60. The Chief Executive Officer, Standard Chartered Bank
61. The Chief Executive Officer, Tropical Bank
62. The Chief Executive Officer, UGAFODE
63. The Executive Director, Uganda Investment Authority
64. The Inspector General of Police, Uganda Police Force
65. The Chief Executive Officer, United Bank for Africa
66. The Commissioner General, URA
67. The Registrar General, URSB
68. The Chief Executive Officer, Uganda Securities Exchange
69. The Chief Executive Officer, USSD
70. The Chief Executive Officer, UTCL
71. The Chief Executive Officer, WAVE
72. The Chief Executive Officer, WORKSCML
73. The Chief Executive Officer, WorksMVR
74. The Chief Executive Officer, SEAMFIX
75. The Executive Director, KCCA