

Our Ref: P2025-06-0001

Date: 16th June 2025

OPEN LETTER

To: PERSONAL DATA PROTECTION OFFICE (PDPO-UG)

info@pdpo.go.ug

Dear PDPO-Ug,

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

The Digital Agenda Forum writes to you with deep concern regarding the ongoing mass National Identification Number (NIN) renewal process currently being implemented by the National Identification and Registration Authority (NIRA). This process involves the collection of extensive personal and biometric data, including an individual's full name, date and place of birth, details of origin and tribe, names of parents, a passport-style facial photograph, signature, fingerprints, and an iris scan.

We acknowledge the Government of Uganda's ambition to modernise identification systems and enhance service delivery. However, we are gravely concerned about 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.

THE EXPANDING USE OF THE NATIONAL IDENTIFICATION NUMBER

The National ID, and by extension the NIN, has evolved into a de facto universal identifier. It is now required for:

- Opening and operating bank accounts
- Registering businesses
- Accessing government services
- Tax registration and compliance (as the new Tax Identification Number)
- Registration and activation of SIM cards through telecommunications service providers
- Mobile money transactions above one million Uganda Shillings.

The consolidation of identity, economic activity, and public service access into a single national credential raises significant legal and ethical concerns.

LEGAL FRAMEWORK AND POTENTIAL NON-COMPLIANCE

Uganda's **Data Protection and Privacy Act, 2019** provides a robust legal framework for safeguarding personal data. Key provisions include:

- **Section 10:** Protects the right to privacy and prohibits unlawful data processing
- **Section 12:** Requires data to be adequate, relevant, and not excessive
- **Section 13:** Mandates transparency about the purpose, nature, and recipients of data
- **Section 19:** Regulates cross-border data transfers
- **Sections 24 to 33:** Provide data subjects with rights such as access, rectification, erasure, and compensation

Additionally, **biometric data**, including fingerprints, facial images, and iris scans, is considered sensitive personal data. Its collection requires specific justification, purpose limitation, and demonstrable safeguards, such as **Data Protection Impact Assessments (DPIAs)**.

The **Registration of Persons Act, 2015**, which governs NIRA's operations, empowers it to collect certain categories of personal information. However, it remains unclear whether the expansion into advanced biometric collection, particularly the iris scans, falls within the legal limits of NIRA's mandate. This requires urgent clarification.

The recent amendments to the **Tax Procedures Code** which designate the NIN as the Tax Identification Number, further entrench its centrality in state-citizen interactions. Such systemic integration, while possibly intended for efficiency, increases risks of profiling, surveillance, identity theft, and exclusion if not adequately regulated.

UGANDA'S INTERNATIONAL COMMITMENTS

Uganda is bound by **Article 27 of the Constitution**, which guarantees the right to privacy. The country also aligns with global best practices, including the **OECD Privacy Guidelines** and the spirit of the **EU General Data Protection Regulation (GDPR)**. These frameworks classify biometric data as "special category" and require higher thresholds for its processing, including necessity, proportionality, transparency, and data minimisation.

COMMENDABLE WORK BY THE PDPO

We commend the Personal Data Protection Office for taking proactive measures to enforce data protection in Uganda. We particularly note:

- Successful enforcement actions against non-compliant entities, including the Uganda Securities Exchange and several data processors
- Registration of over 3,600 data controllers and processors
- Launch of a Data Protection and Privacy Compliance Toolkit

- Public sensitisation efforts and development of a digital complaints platform and SMS/USSD system for citizen redress

These actions are critical for strengthening Uganda's data governance. However, the scale and sensitivity of the current biometric data collection process demands more visible oversight.

CONCERNS ON INVOLVEMENT OF SERVICE PROVIDERS

We are especially concerned about how data is being handled by third-party institutions requiring the National ID, notably:

- **Commercial banks and their agents**
- **Telecommunications companies and their agents** for SIM card registration, digital onboarding and mobile money transactions of amount above one million Uganda shillings.
- **Tax and revenue authorities**
- **Business registration and licensing bodies**

It remains unclear whether these institutions:

- Provide legally compliant privacy notices
- Have conducted DPIAs
- Limit their data collection to necessary categories
- Have appropriate data retention and sharing policies

OUR FORMAL REQUESTS

Given the above, we respectfully make the following requests to the Personal Data Protection Office:

1. Clarify why there appears to be an overcollection of personal 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.
2. Confirm whether DPIAs have been conducted by NIRA and the associated institutions and whether they are publicly available.
3. Clarify whether the current biometric data collection falls within NIRA's mandate under the Registration of Persons Act.
4. Confirm whether the PDPO has issued or intends to issue any guidance regarding the integration of the NIN across essential services.
5. Provide assurance that all third-party institutions requiring the National ID, particularly banks and telecom operators are registered with your office, have appointed Data Protection Officers, and are compliant with the law.
6. Publicly share any data-sharing agreements and security safeguards relating to the current NIN collection and usage.

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

WHY THIS OPEN LETTER

We have chosen to make this a public letter because the matters it raises affect millions of Ugandans whose personal data is being collected, often repeatedly and without clear justification, across various institutions and services. Many are unaware of their rights or lack the means to question these practices. As such, this letter is written not only to seek accountability from the relevant authorities, but also in solidarity with all Ugandans whose data and dignity deserve protection.

CONCLUSION

The people of Uganda deserve an identity system that enhances access to services without compromising their fundamental rights. While we acknowledge the progress your office has made, the nature and extent of data being collected through the NIN renewal process calls for heightened scrutiny, enforcement, and public transparency.

We kindly request a written response addressing the above concerns and indicating the steps being taken to ensure full compliance with the law.

We remain available for constructive engagement on this matter and look forward to your response.

Yours faithfully,

DIGITAL AGENDA FORUM

CC: Permanent Secretary, Ministry of ICT and National Guidance

National Information Technology Authority, Uganda (NITA-U)

National Identification Registration Authority (NIRA)