The Presidency

NATIONAL IDENTITY MANAGEMENT COMMISSION

Proposed Privacy Policy

Final Draft Version No. 1 Approved for Public Circulation and Review
25th June 2010

Introduction

The National Identity Management Commission, following the adoption of the National Policy and Institutional Framework for an Identity Management System for Nigeria, was established under the National Identity Management Commission Act No. 23 of 2007 and charged with the function amongst others to create, manage, maintain and operate the National Identity Database which shall contain registered information or data relating to citizens of Nigeria and non-Nigerian citizens recognized as registerable persons within the meaning of Section 16 of the Act. The National Policy objective was driven by the need, amongst others, to:

- create an effective and efficient identity management system that will, among other benefits, promote e-governance, drive consumer credit system and boost national security in Nigeria; and

- facilitate the provision of a secure and reliable method for ascertaining, obtaining, maintaining and preserving information and facts about citizens of Nigeria and registerable persons.

In light of the privacy implications inherent in the operation and management of an identity management system, the National Policy objective also focused on the need for identified technologies, business practices, law and policies that would, amongst others, enhance security of identity information; preserve and improve upon individual privacy.

Policy Statement

NIMC has identified this policy as a necessary tool for ensuring that privacy rights are protected in the collection of registerable information; operation and management of the Database. To this end, NIMC is committed to safe-guarding the privacy of registered persons by:

- ensuring the security of information or data collected and held in the Database;
- guarding against unauthorized disclosures;
- ensuring that usage of such information or data is limited to only those purposes sanctioned by the Act; and
- disclosure and or use, except for national security interests, is preceded by consent of the individual before or during access and or use.

Definitions

For the purposes of this policy, the definitions of words, terms or phrases contained in Appendix A of this policy shall apply.

Policy Objectives

This policy is designed to ensure that NIMC meets its obligations under the Act in the management of information or data collected and held in the Database. This objective includes ensuring the protection of such information or data by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, storage or disposal.

Expected Results of this Policy

The expected results of this policy include:

- sound management practices with respect to the handling and protection of registered information;

- accountability and responsibility in managing the operation of the Database and the reasonable expectation of privacy by those affected by the Act, including accurate and timely responses to registered persons who may wish to confirm or seek the correction of their personal information held in the Database; and

- identification, assessment and mitigation of privacy impacts and risks for all new or significantly modified identity management projects, services or activities that involve the collection, processing, storage, use or disclosure of registered information.

Application of this Policy

This policy applies to:
- all employees of NIMC;
- all registered information; and
- any other person or third party as may from time to time be designated by NIMC.

Policy Directives

- This policy will be posted on the NIMC web-site at www.nimc.gov.ng

- All employees will be advised of the policy coming into force. All departmental heads and zonal heads in all offices of NIMC throughout the federation shall effective from that date ensure that a copy of this policy is read by members of staff/employees in their respective departments/zones. Evidence of this shall be by way of a form signed by such members of staff/employees confirming that the staff/employee signing the form – has read this policy.

- NIMC will collect, access, store, use, and disclose registered information only in the manner and for the purposes authorized by the Act.

- NIMC has completed a PIA of the National Identity Database project and will complete PlAs for all new or significantly modified projects, activities or services that involve the collection, use or disclosure of registered information.

- NIMC will ensure that agreements entered with any private or public sector based agency or organization for the development or establishment of the Identity Management Solution or for the realization of any of the functions of NIMC are compliant with this policy.

- NIMC will maintain secured communication links with existing relevant identity related database or agency; and with approved end users of registered information in any public or private organization, agency or body including Card Acceptance Devices and Government Service Centres.

- NIMC will establish and implement formal and effective systems/procedures/processes for:
    - collecting and dealing with the information and data of individuals;
    - verifying any registered information or information intended to be entered into the Database;
    - responding to requests made by registered persons for the verification or correction of their registered information; and
    - documenting deliberations and decisions made concerning such requests received under the Act;

  in such a way as to ensure the protection of their privacy rights within the ambit of the Act and the Constitution.

Nature of Information that NIMC is Authorized to Collect

As a matter of policy, NIMC will collect and enter in the Database only those information and data of individuals that are authorized under Section 17 and the Second Schedule of the Act. These include:

- the individual's full name;
- other names by which the person is or has been known;
- date of birth;
- place of birth;
- gender;
- the address of the individual's principal place of residence in Nigeria;
- the address of every other place in Nigeria where the individual has a place of residence;
- a photograph of the individual's head and shoulders;
- the individual's signature; the individual's fingerprints;
- other biometric information about the individual;
- the individual's residential status;
- the individual's National Identity Number; (to be issued by NIMC)
- any national insurance number allocated to the individual;
- any Nigerian or foreign passport number of the individual; (if available)
- driver's license number; (if available)
- record of any changes in the individual's recorded information;
- ID registration and history of such registration;

- validation information (including the individual's password or code for such validation purposes); and
- the date of the individual's death.

Collection of Personal Information

NIMC will collect personal information and data directly from individuals as a requirement for registration for the national identity card. NIMC will not collect personal information about individuals through an unlawful means or by means that are in the circumstances unfair or intrude to an unreasonable extent upon the personal affairs of the individual concerned.

NIMC may adopt methods other than the one used in the ordinary course of registration to confirm the validity of information provided to it by individuals.

Use of Information

The purposes of the information/data collected and stored in the Database are consistent with the reasons for the creation of the Database. These include:

- to facilitate identity authentication;
- to boost national security in Nigeria;
- to assist research efforts and economic planning by Government or agencies;
- to encourage and drive consumer credit system and economic development;
- to prevent identity theft; and
- to assist criminal investigation.

NIMC will establish and implement procedures to ensure that only requests by duly authorized persons/agencies for lawfully authorized use of information and data held in the Database are granted.

Criminal punishment for unlawful use/disclosure of Registered Information

This policy recognizes and affirms that unlawful access or use of information or Data held in the Database by any person, including employees of NIMC, is a criminal offence punishable by imprisonment for a term not less than ten years without the option of fine under the provision of section 28(1) and (2) of the Act.

General Multipurpose Card (GMPC) issued by NIMC to registered persons will contain certain prescribed information or data (albeit in encrypted form as the Act requires). This policy recognizes and affirms that it is the duty of a registered person to secure the safety and preservation of his GMPC in good form and to notify NIMC if the person knows or has reason to suspect that the GMPC has been lost, stolen, damaged, tampered with or destroyed.

Security of Information

NIMC and its employees will make reasonable efforts; establish measures, processes and procedures to ensure the protection of registered information. These include both physical and electronic/technological safeguards. For example:

- information and data contained in the Database will be held in encrypted form/password protected;

- passwords/access codes to registered information/Database will be limited and given to only employees who need access for a lawfully authorized purpose and compliance will be duly monitored on an on-going basis;

- procedures and measures/technologies will be put in place to provide monitoring of the Database and ensure that there is evidence of, and audit trail to reveal without ambiguity, the person/status of the person accessing the Database, time of accessing and the specific information viewed, accessed, or retrieved from the Database; and

- employees, as a general policy, must keep filing cabinets/personal computers containing any official information or document duly locked/passworded at all times and no such files must be left unattended.

Caveat

The collection, storage or transmission of any information/data electronically or via the internet is not completely secure and therefore NIMC cannot guarantee and does not take or accept responsibility for the security of information/data transmitted electronically.

NIMC does not accept responsibilities for any reliance on any links to third party websites that may be found on NIMC's websites or any reliance on such third party's policies as NIMC has no control over them.

Disclosure of Information

NIMC will take reasonable efforts to create and maintain firewalls, restricted access and other appropriate safeguards to ensure that to the extent that it controls registered information, it is dealt with only in the manner authorized by the Act.

NIMC will not disclose or authorize the disclosure of any registered information except:

- the disclosure is authorized by or consented by the registered individual concerned; or
- the disclosure is required in compliance with a court order; or
- the disclosure is made to a designated and specified judicial or police authority in the public interest; or
- such disclosure is authorized by the Act, if the disclosure is:
    - in the interest of National Security; or
    - necessary for purposes connected with the prevention or detection of crime; or

- for any other purpose, strictly in the public interest, specified by NIMC in a regulation;

Amendments to Policy

This policy may be amended at any time. Amended versions shall be duly posted on NIMC's official web-site and given same treatment as contained under item 2 of Policy Directives.

Enquiries

Please direct enquiries about this policy to:

The Director General / Chief Executive
National Identity Management Commission
11 Sokode Crescent, Off Dalaba Street
Zone 5, Wuse
P. M. B. 18, Garki – Abuja

Phone: +234-9-6726456
E-mail: **pia@nimc.gov.ng**

www.nimc.gov.ng

Miscellaneous

In the event of any discrepancy or conflict between this policy and the provisions of the Act or any Regulations thereto or Orders/Directives of the Federal Executive Council of Nigeria; the provisions of the Act/Regulations or the said Orders/Directives shall take precedence over this policy.

Appendix A

Definitions

The definition of words, terms or phrases contained herein shall apply to this policy:

Act	National Identity Management Commission Act, No 23 of 2007.
Biometric information	as defined in the Act, in relation to a registered individual, means data about such individual's external characteristics, including in particular, the features of an iris or any other part of the eye.
Database	as defined in the Act, means the National Identity Database established pursuant to section 14 of the Act.

Employee	an individual in the employ of, seconded to, or under personal service contract to NIMC and includes their volunteers, National Youth Service Corp members engaged with NIMC; and interns who have or may have access to any registered information.
Fingerprint(s)	as defined in the Act, in relation to a registered individual, means a record (in any form and produced by any method) of the skin pattern and other physical characteristics or features of any of the individual's fingertips.
National Policy	National Policy and Institutional Framework for an Identity Management System for Nigeria
NIMC	National Identity Management Commission established under Section 1(1) of the National Identity Management Commission Act, No 23 of 2007.
PIA	Privacy Impact Assessment – an exercise carried out to determine and assess the risks of privacy interference as well as identify remedial steps necessary to improve privacy protection.
Privacy	the claim of an individual or individuals to determine for themselves when, how and to what extent information about them is communicated to others.
Registered information	as defined in the Act, means in relation to any registered individual, the information and data, including biometric information entered into the Database in respect of the individual.
Registered person	any individual whose registered information has been entered in the Database.