



16th March 2026

Our Ref: NIA-R/ES/V2/199

NIA GUIDELINE NO. 1/26

GUIDELINES FOR USER AGENCIES ON THE SECURITY, STORAGE AND RETENTION OF PERSONAL INFORMATION OBTAINED FROM THE NATIONAL IDENTIFICATION REGISTER (NIR)

Issued by the National Identification Authority (NIA) pursuant to Sections 59 and 61 of the *National Identity Register Act, 2008 (Act 750)*, as amended by the *National Identity Register (Amendment) Act, 2017 (Act 950)*

1. Introduction

These guidelines are issued in accordance with Sections 59 and 61 of the *National Identity Register Act, 2008 (Act 750)*, as amended by the *National Identity Register (Amendment) Act, 2017 (Act 950)*, which mandate the National Identification Authority (NIA) to provide guidance to user agencies on the storage, security, retention and disposal of personal information obtained from the National Identity Register (NIR) and prescribe retention periods for personal information used by user agencies for administrative purposes.

These guidelines seek to:

- a) Ensure that personal information is stored and retained securely and only for as long as necessary;
- b) Promote responsible management of personal information;
- c) Minimize the risks of unauthorized access, misuse, or loss of data; and
- d) Ensure compliance with Ghanaian law and alignment with international standards on data protection and information security.

2. Legal Basis

Section 59: "Where a user agency holds personal information, it shall secure and store the information in accordance with guidelines issued by the Authority."

Section 61: "Where a user agency uses personal information for an administrative purpose, it shall retain the information after its use for the period contained in guidelines issued by the Authority."

3. Definitions

User Agency – includes the Social Security and National Insurance Trust, the National Health Insurance Authority, the Ghana Revenue Authority, the Ghana Immigration Service and any other public or private organisation approved of by the Minister which requires identity data from the NIA.

Personal Information – information or data about an identifiable individual that is recorded in any form including (a) information that relates to the nationality, age or marital status of the individual, (b) information that relates to the educational level, or occupation of the individual or information that relates to a financial transaction in which the individual has been involved, (c) an identification number, symbol or other particulars assigned to the individual, and (d) identity data;

Storage – The act of maintaining personal information in physical or electronic form.

Retention Period – The approved length of time a User Agency may hold personal information for administrative purposes.

Disposal – Secure and irreversible deletion or destruction of personal information.

4. Principles Governing Retention and Disposal

4.1 Purpose Limitation

Personal information shall only be retained for as long as necessary to fulfil the administrative purpose for which it was collected.

4.2 Data Minimization

User agencies shall only retain the minimum necessary data and for the shortest possible time, consistent with the purpose of processing.

4.3 Security of Retained Data

Personal information must be stored securely, with access restricted to authorized personnel and protected using technical and organizational safeguards.

4.4 Disposal Obligation

Personal information must be disposed of promptly once the retention period expires, unless otherwise required by law or regulation.

5. Core Principles

5.1. Security and Storage (Section 59)

User Agencies shall:

- a. Store personal information in secure environments, whether physical or digital;
- b. Implement technical and organizational security measures, including:
 - i. Access controls,
 - ii. Encryption,
 - iii. Secure backups,
 - iv. Protection against unauthorized access, loss or breach
- c. Use secure servers hosted in-country or in jurisdictions with strong data protection regimes;
- d. Ensure physical files are stored in locked cabinets, rooms with restricted access, and areas protected against fire, flood, theft or other perils;
- e. Perform periodic risk assessments and update security controls accordingly.

5.2 Retention and Disposal (Section 61)

User Agencies shall:

- a. Retain personal information only for the period necessary to fulfil the specified administrative purpose;
- b. Ensure timely and secure disposal once data is no longer required;
- c. Maintain audit trails and documentation on data lifecycle management.

6. Standard Retention Periods

Unless specified otherwise by a sector-specific law, the following shall apply:

Data Use Purpose	Maximum Retention Period	Comments
Verification of Identity	Six (6) months	For one-time or limited-purpose identity checks
Ongoing service provision (e.g. banking, insurance, health, taxation)	Duration of the service plus two (2) years	A 2-year grace period allows for dispute resolution, audits or legal compliance
Employment background checks and vetting	One (1) year	After which data must be anonymized or deleted
Regulatory compliance (e.g. KYC, AML)	Five (5) to Seven (7) years	Subject to sector regulations

Data Use Purpose	Maximum Retention Period	Comments
Research or statistical purposes	Indefinite	Must meet anonymization standards; personal identifiers must be removed

Note: If legal or regulatory obligations require longer retention, the user agency must document the justification and inform the NIA accordingly.

7. Secure Disposal Procedures

When retention periods expire, and data is being disposed of, user agencies must:

- a) Use secure deletion tools that meet industry standards (e.g., NIST 800-88 or ISO/IEC 27040 or equivalent).
- b) Shred, incinerate or pulp documents using approved methods.
- c) Maintain audit logs of all data disposal activities for a minimum of twelve (12) months.
- d) Ensure third-party vendors involved in data disposal are vetted and bound by data protection obligations.

8. Documentation and Compliance

User Agencies must:

- a) Keep a Data Retention and Disposal Policy.
- b) Maintain a Retention Schedule detailing:
 - i. Categories of data held
 - ii. Retention periods
 - iii. Disposal methods
 - iv. Responsible officers
- c) submit to the NIA an Annual Data Retention Compliance Report no later than 31st January of each calendar year, in respect of the preceding year or such other date as the NIA may prescribe in writing;
- d) failure to submit the report within the stipulated period shall constitute a breach of these Guidelines and may attract sanctions in accordance with applicable NIA Guidelines or relevant law.

9. Exceptions and Special Circumstances

Where a User Agency has a lawful basis for retaining data beyond the periods specified, they must:

- a) Obtain prior written authorization from the NIA;
- b) Justify the extension with legal or operational reasons; and

- c) Demonstrate that extended retention does not infringe on the rights of data subjects.

10. Enforcement and Compliance Measures

- a) Where a user agency fails to comply with retention and disposal guidelines, the NIA may:
 - i. conduct a compliance review or audit of the user agency's data management practices;
 - ii. issue corrective directives requiring remedial action within a specified period; and
 - iii. where appropriate, refer the matter to the Data Protection Commission or other competent authority for further action under applicable law.
- b) Without prejudice to paragraph (a), and subject to due process, such non-compliance may result in one or more of the following administrative measures:
 - i. Revocation or Suspension of access to the National Identity Register - failure to adhere to retention, security or disposal guidelines may lead to revocation or suspension of the user agency's access to the National Identity Register (NIR), the Identity Verification System Platform of the NIA or other critical systems, subject to notice and opportunity to remedy;
 - ii. Termination of access where persistent or material non-compliance continues after reasonable notice and opportunity to remedy;
 - iii. Imposition of conditions requiring the user agency to implement corrective or remedial measures as a prerequisite for continued access to NIA systems;
 - iv. Legal Action and Liability – Non-compliance shall lead to civil or criminal liability under the *Data Protection Act, 2012 (Act 843)*, with regard to data breaches, misuse or unauthorized access. User Agencies may be liable to compensate individuals affected by improper handling or retention of their personal information. Any criminal liability, fines or penalties arising from non-compliance with data protection obligations shall be determined in accordance with the *Data Protection Act, 2012 (Act 843)* and other applicable enactments;
 - v. Requirement to remedy data breaches, including implementing corrective actions or notifying affected individuals;
 - vi. Order to cease unlawful processing of data; and
 - vii. Where a finding of non-compliance has been made by a competent authority, the NIA may, where appropriate and in the interest of transparency, publish the outcome of such findings in accordance with law.

11. Review and Updates

These guidelines shall be reviewed every three (3) years, or earlier if required by legal or technological changes and updated accordingly by the NIA.

12. Effective Date

These guidelines come into force on 19th March 2026, and shall be binding on all user agencies that access data from the National Identity Register.

Signed,



Wisdom Kwaku Deku
Executive Secretary
National Identification Authority

To all authorised user agencies that receive or process personal information from the National Identity Register

Cc: All Governing Boards/Councils/MDAs