



**DATA PROTECTION  
AND MANAGEMENT  
POLICY STATEMENT**

|                                 |   |
|---------------------------------|---|
| <b>Policy Version Reference</b> | 2024_1.0  |
| <b>Policy Approver</b>          | AGF Board of Directors, following the recommendation of the Audit and Risk Committee. |

# 1. Introduction

The African Guarantee Fund (AGF) is a Pan-African non-bank financial institution whose primary mandate is to assist financial institutions (FIs) in Africa to scale up their SME financing initiatives.

AGF contributes to the promotion of economic development, vital for the prosperity, stability and poverty reduction in Africa through provision of a mix of financial guarantees and other products which will reduce the risks supported by financial sector lending to SMEs that have insufficient collateral and support for capacity development of the partner financial institutions.

**AGF is rated 'AA-' by the globally renowned Fitch Ratings Agency.**

## 2. Purpose

The purpose of this Policy is to ensure data security and privacy in line with applicable laws & regulations and international best practices and standards.

## 3. Scope

The Policy applies to all employees, directors (Board members), officers, contractors, consultants, and partners of AGF, regardless of their role or level within the organization or business relationship with AGF. It governs our conduct in all business activities, interactions with colleagues and stakeholders, and engagement with the communities in which we operate.

## 4. Our Responsibilities

At African Guarantee Fund (AGF), we are committed to ensuring the highest standards of data protection and management across all levels of our organization. The organization is committed to safeguarding the privacy and security of all data it collects, processes, or stores.

It is the responsibility of the organization to:

- Ensure compliance with applicable data protection laws and regulations.
- Implement robust data management procedures that ensure accuracy, confidentiality, and security of both personal and non-personal data.
- Take proactive measures to prevent data breaches and mitigate risks to data security.
- Provide training and awareness programs to all employees to uphold data protection standards.
- Establish clear procedures for handling, storing, and disposing of data in a responsible and compliant manner.
- Regularly review and update data protection practices to ensure they remain effective and aligned with evolving regulatory requirements.

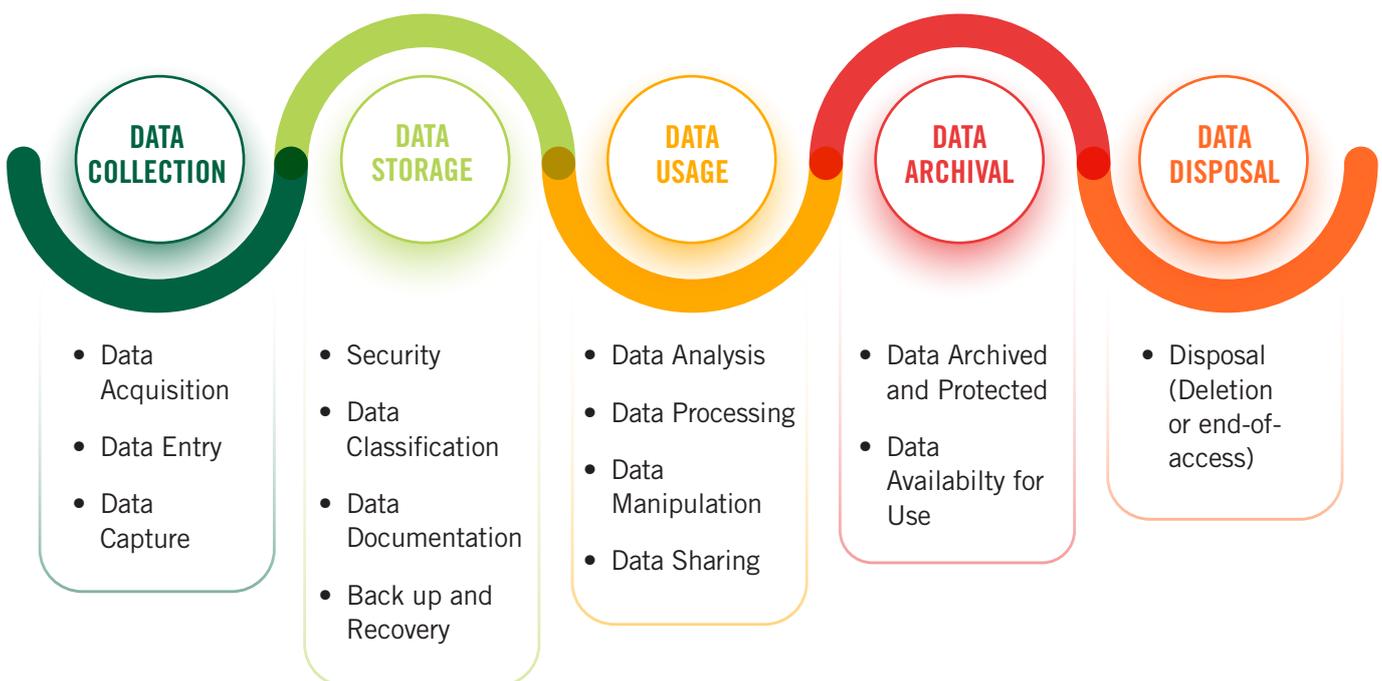


## 5. AGF Data Protection and Management Guiding Principles

### 5.1 Data Management Policies

We conduct Data Protection Impact Assessments (DPIAs) to identify and mitigate potential privacy risks, implementing appropriate measures and controls to ensure efficient and secure data management.

AGF is committed to ensuring appropriate controls, and best practices are implemented throughout the data lifecycle.



## 5.2 Data Protection Policies

We operate a 'Privacy by Design' approach and ethos, with the aim of mitigating the risks associated with processing personal data through prevention via our processes, systems, and activities.

To uphold this commitment, we implement measures such as data;

- Minimization
- Pseudonymization
- Encryption and partitioning
- Hard Copy securely store in safe
- Classification with adequate access right

We are committed to ensuring that any data collected, processed, or shared, either sensitive personal or not, is processed lawfully, fairly, and transparently, with a clear legal basis for each processing activity. Third-party processors are thoroughly assessed for compliance with data protection laws, and contracts outline their data protection obligations.

Data is retained only as long as necessary to fulfill its purpose, with retention periods clearly documented. Once data is no longer needed, it is securely disposed of to prevent unauthorized access, ensuring compliance with relevant laws and protecting individual privacy.

AGF commits to prepare a robust data breach response plan in place to manage and mitigate the impact of data breaches. Breaches are promptly reported to the Supervisory Authority and affected individuals, and corrective actions are implemented to prevent future breaches, ensuring the security and integrity of personal data.





## 5.3 Data Subjects Rights Policies

AGF is committed to upholding data subject rights by taking appropriate measures to ensure consent is obtained for both internal and external data processing activities. We recognize and respect the rights of individuals to control their personal data.

Our policies ensure that consent is freely given, specific, informed, and unambiguous, with transparent requests that are easy to understand. We process employee data based on contractual and legal obligations, ensuring employees are informed about how their data is used and their rights. Individuals have the right to access their personal data, obtain information about how it is processed, and request corrections if it is inaccurate or incomplete.

We respect the right to erasure, allowing individuals to have their data deleted when it is no longer necessary. Additionally, individuals can request the restriction of their data processing under certain conditions and have the right to data portability, receiving their data in a structured, machine-readable format. We recognize the right to object to data processing for specific purposes, such as direct marketing, and ensure that individuals are informed about their rights regarding automated decision-making and profiling.

## 5.4 External Policies

AGF maintains an external privacy policy that covers essential data practices beyond privacy, secures acknowledgment from relevant stakeholders, and complies with current regulatory standards. The external policy provides information on data rights and legal protections in accordance with data protection laws in Kenya, Mauritius, and Togo (“Data Protection Laws”).

When entering into a relationship with external stakeholders, it is essential to recognize, review and monitor their policies, particularly those that may impact or interact with our own data management and protection protocols.

**For more information please refer to our [External Data Privacy Policy](#) available on our website.**

## 5.5 Sanctions

AGF takes compliance with the data management and protection policy very seriously. Failure to comply with the policy:

- Puts data subjects at risk.
- Carries the risk of significant civil and criminal sanctions for the individual and AGF; and
- May, in some circumstances, amount to a criminal offence by the individual.

Employees will be made aware of the severity of such penalties and their proportionate nature in accordance with the breach. We recognize that:

- Breaches of the obligations of the controller, the processor, the Supervisory Authority, basic principles for processing, conditions for consent, the data subjects' rights, the transfers of personal data to a recipient in a third country or an international organization, specific processing situations or general non-compliance with the Data Protection Act are subject to administrative fines.
- Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect. Employees are at liberty in case of any questions or concerns about this policy, to contact the Data Protection Officer.





Africa House, Muthangari Road  
Nairobi, Kenya

**Tel:** +254 732 148 000

**Web:** [www.africanguaranteefund.com](http://www.africanguaranteefund.com)