ACCESS TO FINANCE RWANDA

AFR
Privacy Policy

ACCESS TO FINANCE RWANDA

Privacy Policy

Date of revision	22nd March 2025
Policy owner	Chief Operations Officer (COO)
Status	Public

Versions Control

Versions	**Description of Change implemented**	**Submitted by**	**Reviewed by the Finance, Audit and Risk Committee on**	**Approved by the Board on**
Version 1	Data Protection Policy	COO	12th August 2021	28th October 2021
Version 2	AFR Privacy Policy (Repeal and replacement of data protection policy)	COO	18th March 2025	22nd March 2025

List of Contents

1. Introduction

At **Access to Finance Rwanda** (hereafter "**AFR**", "we", "us", "our"), we are committed to safeguarding the privacy and security of the personal data entrusted to us by our Board, employees, stakeholders, and partners. This internal privacy policy outlines the comprehensive measures we have in place to protect and manage the data we handle in our daily operations. Recognising the importance of data protection in today's digital landscape, our commitment extends beyond mere compliance with regulations to a proactive and ethical approach to ensuring the confidentiality, integrity, and availability of the information we process.

2. Policy Statement

AFR is committed to complying with all relevant Rwandan legislation and applicable global legislations. AFR recognises that the protection of individuals through lawful, legitimate, and responsible processing and use of their personal data is a fundamental human right. AFR will ensure the protection of data subjects' rights and that all data collection and processing activities comply with the relevant legislation. AFR staff must comply with this policy, breach of which could result in disciplinary action.

3. Scope

The policy applies to:

- Employees of AFR and all AFR's associated parties such as members of the Board, implementing partners, vendors, contractors and any other third parties who handle and use AFR information (where AFR is the 'Controller' for the personal data being processed, be it in manual and automated forms or if others hold it on their systems for AFR;
- All personal data processing AFR carries out for others (where AFR is the 'Processor' for the personal data being processed) and,
- All formats, e.g., printed and digital information, text and images, documents and records, data and audio recordings.

4. Purpose

The policy offers guidance on how AFR will manage the data it collects, ensuring compliance with data protection laws, safeguarding data subjects' rights, and mitigating risks associated with data protection breaches.

5. Definitions

Organisation	Access to Rwanda Finance (AFR)
RDPA	means the Rwandan Law Nº 058/2021 of 13/10/2021 relating to the protection of personal data and privacy (RDPA)
Responsible Person	Data Protection Officer (DPO)
Data Protection Officer	The primary role of the data protection officer (DPO) is to ensure that the organisation processes the personal data of its Board, staff, stakeholders, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules
Personal Data	Any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person.
Sensitive Personal data	Information revealing a person's race, health status, criminal records, medical records, social origin, religious or philosophical beliefs, political opinion, genetic or biometric information, sexual life or family details.
Processing of personal data	An operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as access to, obtaining, collection, recording, structuring, storage, adaptation or alteration, retrieval, reconstruction, concealment, consultation, use, disclosure by transmission, sharing, transfer, or otherwise making available, sale, restriction, erasure or destruction.
Privacy	A fundamental right of a person to decide who can access his or her personal data, when, where, why and how his or her personal data can be accessed.
Data subject	A natural person from whom or in respect of whom, personal data has been requested and processed.
Data Controller	Natural person, public or private corporate body or legal entity which, alone or jointly with others, processes personal data and determines the means of processing.
Data Processor	Natural person, public or private corporate body or legal entity, which is authorised to process personal data on behalf of the data controller.
Competent authority	Sectoral authority responsible for overseeing sector-specific compliance in conjunction with the supervisory authority.
Supervisory authority	A public authority in charge of cyber security.
Person	Natural person, corporate body, or legal entity.

6. Principles

AFR is deeply committed to the ethical and responsible processing of personal data in compliance with the principles set forth by the RDPA and we take every possible measure to ensure that the following principles are adhered to.

i. Lawfulness, Fairness, and Transparency:

- **AFR** will ensure that data is processed lawfully, fairly and in a transparent manner and in line with the right to privacy.
- **AFR** will always establish a valid legal basis as outlined in the RDPA. All departments of the business will document and maintain the lawful basis for processing personal information across all processes and operations. The legal basis is documented in detail in section 10 of this policy.
- **AFR** will strive to treat data subjects' personal data with fairness and respect. This entails providing information to data subjects about how **AFR** processes their data through clear and concise privacy notices.

ii. Purpose Limitation:

- **AFR** will, at all times, collect, use personal information for specific purposes only, and a record of these purposes will be documented and maintained by the department making use of the personal data.
- Personal data are not to be further processed in a manner incompatible with that purpose.

iii. Data Minimisation:

- **AFR** will collect and process only the minimum amount of personal data necessary to achieve the specified purposes.
- **AFR** staff must not access data which they are not authorised to access nor have a reason to access.
- Data must only be collected for the performance of duties and tasks; staff must not ask data subjects to provide personal data unless that is strictly necessary for the intended purpose.

iv. Accuracy:

- **AFR** will take reasonable steps to ensure that all personal data and information is kept accurate, complete, up to date, and not misleading as is necessary for the purposes for which it is processed.
- All relevant records must be updated should staff be notified of inaccuracies. Inaccurate or out of date records must be deleted or destroyed.

v. Storage Limitation:

- **AFR** is committed to implementing effective mechanisms for retaining and disposing of personal data. The establishment and maintenance of retention schedules consider legal, regulatory, and business requirements, prioritising the principle of not retaining personal data longer than necessary.

- Refer to our Record Management Procedure for more information on personal data retention and disposal.

vi. Rights of Data Subjects:

- We will process personal data in compliance with the rights of the data subjects.

7. Accountability

AFR recognises itself as a responsible data controller under the RDPA. Hence, we are committed to complying with the requirements laid down in Article 38 of the RDPA as follows:

- To implement appropriate technical and organisational measures;
- To maintain a record of processing operations;
- To carry out privacy assessments when the processing of personal data is likely to pose a high risk to the rights and freedoms of the data subjects;
- To perform such other duties as assigned by the supervisory authority.

Roles and Responsibilities

S/N	Members	Role
1	CEO COO	The CEO and COO will provide overall leadership and support for data protection initiatives, ensuring data protection is integrated into **AFR**'s strategic objectives.
2	Board	The Board will provide governance oversight of activities under this policy and will ensure that there are adequate and effective systems and process in place to safeguard data.
3	Data Protection Officer ("DPO")	The DPO will act as the main point of contact for data protection matters and provide expertise on regulatory compliance and report to the CEO.
4	Human Resources Manager	The Human Resources Manager will ensure that data protection principles are integrated into HR policies and procedures, particularly concerning employee data and work on a training program on data protection and security measures.
5	Head of Finance and Grant Management	The latter will oversee the financial aspects of data protection initiatives and budget allocation for necessary resources.
6	Legal Counsel/ Advisor	This member will advise the committee on legal aspects of data protection, ensuring the **AFR**'s practices align with relevant laws and regulations.

7	Other relevant head of departments	Representatives from different departments are responsible for: • ensuring staff and third parties they work with are aware of the contents of this policy • the management and processing of personal data • participating in the committee to provide insight into their specific data protection needs and challenges • conducting risk assessments and updating controls and procedures to mitigate the risk of data breaches.
8	All Staff	Read, understand and comply with the contents of this policy. Report suspicions of breaches promptly.
9	Grantees or partners	Grantees and partners of **AFR** must report breaches of **AFR**'s data in their custody within 24 hours using the emails provided below. Grantees and partners must also abide by this policy and institute adequate mechanisms to safeguard the privacy of individuals data.

8. Data Protection Officer

We have appointed a DPO to oversee and ensure compliance with the RDPA. The contact details of the DPO of **AFR** are as follows:

- **Name**: Allan Mugabi
- **Email:** dataprotection@afr.rw
- **Telephone:** +250 782 507 751

The duties of the DPO are as follows:

- To inform and advise **AFR** and its employees who carry out personal data processing, of their obligations pursuant to the RDPA;
- To monitor, in his or her area of work, compliance with the RDPA and with the policies of **AFR** in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in personal data processing operations, and the related audits;
- To provide advice where requested as regards to the data protection impact assessment and monitor its performance;
- To cooperate with the supervisory authority and to act as its contact point on issues relating to the processing of personal data, including the prior consultation with the supervisory authority, and to consult, where appropriate, with regard to any other matter.

- To monitor, in the area of work, compliance with the RDPA and with the policies of the data controller or data processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in personal data processing operations and the related audits.
- To provide advice where requested, with regards to the data protection impact assessment and monitor its performance.
- To cooperate with the supervisory authority and to as its contact point on issues relating to processing of personal data, including the prior consultation with the supervisory authority, and to consult where appropriate, regarding any other matter.

9. Registration with the supervisory authority

Article 29 and 33 of the RDPA require the following:

- Under Article 29, every data controller or data processor must register with the supervisory authority. The supervisory authority puts in place a register of data controllers and data processors.
- Under Article 33, the data controller or the data processor who holds a registration certificate may apply for its renewal within forty-five (45) working days before the expiry date of the existing certificate.

AFR is registered with the supervisory authority and the registration numbers are as follows:

- **Data Controller registration No:** [001/0279/0837]
- **Data Processor registration No:** [002/0064/0923]

10. Lawful basis of processing personal data

At the core of all personal data processing activities undertaken by **AFR**, is the assurance and verification that we are complying with Article 46 of the RDPA and our lawfulness of processing obligations. Prior to carrying out any processing activity on personal information, we always identify and establish the legal basis for doing so and verify these with the data protection laws.

This legal basis is documented on our Record of Processing Activties sheet and where applicable, is provided to the data subject and the Data Protection Office as part of our information disclosure obligations. The lawful bases which **AFR** will rely on for processing personal data are where:

- The data subject has given consent to the processing of their personal data for one or more specific purposes;
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- Processing is necessary for compliance with a legal obligation to which we are subject;
- Processing is necessary for the purposes of the legitimate interests pursued by **AFR** or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data).

11. Consent

Where consent is relied upon as a lawful basis for processing data, evidence of the consent shall be kept with the personal data. Where communications are sent to individuals based on their consent, the option for the individual to withdraw their consent should be clearly available and systems should be in place to ensure such withdrawal is reflected accurately in our systems.

Where necessary, AFR will maintain adequate records to show that consent was obtained before personal processing data. Data will not be processed after the withdrawal of consent by a data subject.

12. Processing sensitive personal data

AFR recognises that certain categories of personal data are classified as sensitive personal data and that the processing will be strictly conducted in accordance with the RDPA. We will only process special categories of personal data where:

- The data subject has given explicit consent to the processing of the personal data;
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or exercising specific rights of the data subject in accordance with relevant laws;
- Processing is necessary to protect the vital interests of the data subject or of any other person;
- Processing is necessary for the purposes of preventive or occupational medicine, public health such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices;
- Processing is necessary for archiving purposes in the public interest or scientific and historical research purposes or statistical purposes.

Where **AFR** processes personal data that falls into one of the above categories, we have the specified provisions and measures in place prior to any processing.

Measures include:

- Ensuring we are compliant with the requirements for personal data protection or personal data monitoring as required by RDPA;
- Ensuring we are compliant with applicable sensitive personal data retention periods established by RDPA;

  Refer to the Record Management Procedure for more information on the retention periods.
- Implementation of appropriate technical and organisational measures to ensure a level of security appropriate to the risk posed to the data subject, including, where appropriate, storing sensitive personal data separately from other types of data, and applying measures such as tokenisation, pseudonymisation or encryption.

13. Processing data relating to a child

AFR will not process data relating to a child unless consent is given by the child's guardian or parent and the processing is in such a manner that protects and advances the rights and best interests of the child in line with **AFR**'s Safeguarding policy. **AFR** will institute adequate mechanisms to verify the age and obtain consent before processing the data.

14. Duty to notify

AFR has a duty to notify data subjects of their rights before processing data. **AFR** will therefore inform the data subjects of their right:

- To be informed of the use to which their personal data is to be put.
- To access their personal data in **AFR**'s custody.
- To object to the processing of all or part of their personal data.
- To the correction of false or misleading data.
- To deletion of false or misleading data about them

To notify data subjects on how AFR uses their personal data, kindly refer to the privacy notices of AFR.

15. Your Data Subject Rights

We respect the rights of individuals regarding their personal data. Data subjects have the right to access, object to data processing for specific reasons, personal data portability, not to be subject to a decision based on automated data processing, restrict processing of personal data, request for erasure of your personal data when no longer required, update or rectify inaccurate or incomplete data, right to designate an heir to personal data and right to representation, as well as the right to withdraw their consent.

AFR will devise procedures to ensure that data subjects are provided with appropriate information about the processing of their personal data and to meet other applicable obligations to data subjects related to the processing of their personal data.

For more information on how to handle a data subject right request, consult our Data Subjects Rights Request Procedure.

16. Record of Processing Activities (RoPA)

AFR maintains a record of processing activities as provided under Article 17 of the RDPA. This document helps us understand the types of personal data we hold, its sources, the purposes for which it is used, the retention period and relevant lawful basis applicable amongst others.

To maintain an accurate and up to date RoPA, all departments within **AFR** will be responsible for informing the DPO of any changes to the personal data they collect and process.

17. Data Retention & Disposal

AFR has a Record Management Procedure in place to provide guidelines for the retention of personal data and aids employees in understanding their obligations to keep personal data as long as it is necessary and to destroy the personal data once the retention period has lapsed to meet legislative, fiscal, administrative, and operational requirements.

The retention period is also documented in the Record of Processing Activities.

18. Privacy by Design and by Default

AFR adopts a "Privacy by Design and Default" approach to ensure that data protection measures are embedded into systems, processes, and services from the outset. This approach will promote a proactive and privacy conscious culture within **AFR**.

19. Security

Alongside our 'Privacy by design' approach to protecting data, **AFR** takes the security of your personal data seriously and has implemented appropriate technical and organisational measures to protect it from unauthorised access, disclosure, alteration, and destruction. Our security measures include, but is not restricted to:

- Strong password protection
- Access control
- Encryption
- Virus and malware protection
- Firewall
- Audit trail
- Business continuity
- Backup and restoration.
- [AFR to add another security measure]

20. Data Protection Impact Assessment

Individuals have an expectation that their privacy and confidentiality will be upheld and respected whilst their data is being stored and processed by **AFR**. We, therefore, utilise several measures and tools to reduce risks and breaches for general processing, however when the processing is likely to be of high risk or cause significant impact to a data subject, we utilise proportionate methods to map out and assess the impact ahead of time.

Where there is a likelihood that such processing could result in a high risk to the rights and freedom of data subjects, we always carry out a Data Protection Impact Assessment (hereafter "**DPIA**") as per Article 38 of the RDPA. Carrying out DPIAs enable us to identify the most effective way to comply with the RDPA and ensure the highest level of data privacy when processing. It is part of our Privacy by Design approach and allows us to assess the impact and risk before carrying out the processing, thus identifying and correcting issues at the source, reducing costs, breaches and risks.

Please refer to our Data Protection Impact Assessment Procedure for more details.

21. Breach Management

Whilst every effort and measure are taken to reduce the risk of data breaches, **AFR** has established a procedure to promptly respond and manage personal data breaches to comply with the reporting requirement under the RDPA. This procedure is intended to enable **AFR** to contain, assess and respond to data breaches quickly and to help mitigate potential harm to affected individuals in compliance with the RDPA.

Please refer to our Data Breach Response Plan for specific protocols.

22. Processor Selection

AFR may utilise external processors for certain processing activities. We abide by a set of rules and procedures to follow for establishing business relationships with third-party service providers, namely with regard to identifying and assessing vendors as well as evaluating their privacy risk.

To maintain a high standard of data protection, **AFR** has implemented a Vendor Management Procedure which defines requirements for effective management and oversight of vendors from a privacy perspective and sets out the rules and procedures to follow for establishing business relationships with third-party service providers, namely regarding:

- Identifying and assessing vendors;
- Evaluating vendor privacy risk;
- Developing a thorough contract; and
- Monitoring vendors' privacy practices and performance.

Refer to our Vendor Management Procedure which defines requirements for effective management and oversight of service providers from a privacy perspective.

23. Transfer and Data Sharing

AFR takes proportionate and effective measures to protect personal data always held and processed by us, however, we recognise the high-risk nature of disclosing and transferring personal data and as such, place an even higher priority on the protection and security of data being transferred.

Whenever personal data is transferred across borders, **AFR** conforms with the requirements of the data protection laws regardless of the jurisdictions. In other words, we only transfer personal data abroad if adequate protection is ensured, as per Article 48 of the RDPA.

AFR will transfer personal data out of Rwanda only when we have:

1. The authorisation granted by the Authority in charge of data protection and privacy after providing proof of appropriate safeguards with respect to the protection of the personal data; and
2. The data subject has given explicit consent to the proposed transfer, after having been informed of the possible risks of the transfer owing to the absence of appropriate safeguards;
3. The transfer is necessary:
    - For the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
    - For the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person;

- For reasons of public interest as provided by law;
- For the establishment, exercise or defense of a legal claim; or
- In order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or
- For the purpose of compelling legitimate interests pursued by the controller or the processor which are not overridden by the interests, rights and freedoms of the data subjects involved and where:
    - The transfer is not repetitive and concerns a limited number of data subjects; and
    - The controller or processor has assessed all the circumstances surrounding the data transfer operation and has, based on such assessment, provided to the Authority proof of appropriate safeguards with respect to the protection of the personal data; or

4. The transfer is made from a register which, according to law, is intended to provide information to the public and which is open for consultation by the public or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down by law for consultation are fulfilled in the particular case.

A transfer pursuant to paragraph (20)(4) shall not involve the entirety of the personal data or entire categories of the personal data contained in the register and, where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or in case they are to be the recipients.

Paragraph (20)(1) and (3)(i), (ii) and (vi) shall not apply to activities carried out by a public entity in the exercise of its functions as per the Rwanda Data Protection and Privacy Law.

AFR will process sensitive personal data out of Rwanda only after obtaining the consent of a data subject and on receiving confirmation of appropriate safeguards and obtaining authorisation from the data protection and privacy authority.

When personal data is shared with third parties, we enter into data sharing agreements to conform with the provisions of the RDPA where possible.

Refer to sharing agreements such as Controller-Processor Agreement and Data Sharing Agreements.

24. Training

We aim to raise awareness, build a strong data protection culture and foster a sense of responsibility among our employees. Through ongoing training and education that will be planned, our employees will be better equipped to handle personal data responsibly, mitigating data protection risks and ensuring compliance with the RDPA.

25. Independent Assurance

The adequacy and effectiveness of AFR's data protection procedures is subject to the regular internal audit reviews where necessary AFR may call an external review provide assurance over the integrity.

26. Complaints Procedure

All complaints under this Policy can be brought in writing to the DPO. The contact details of the DPO are provided under section 8 of this Policy.

27. Penalties

AFR understands its obligations and responsibilities under the RDPA and comprehends the severity of any breaches under the RDPA. We respect the Supervisory Authority's authorisation under the legislation to impose and enforce fines and penalties on us where we breach the RDPA, fail to mitigate the risks where possible and operate in a knowingly non-compliant manner.

Employees have been made aware of the severity of such penalties and their proportionate nature in accordance with the breach.

We recognise that:

- Under Article 56 of the RDPA, the processing personal data contrary to the RDPA is unlawful,
- Under Article 57 of the RDPA, any person who knowingly, intentionally or recklessly re-identifies personal data which have been de-identified by a data controller or a data processor and/or re-identifies and processes personal data, without consent of the data controller, commits an offence.
- Under Article 58 of the RDPA, destruction, erasure, concealing or alteration of personal data in a way that is contrary to the RDPA is an offence,
- Under Article 59 of the RDPA, sales of personal data in a way that is contradictory to the RDPA is an offence,
- Under Article 60, the collection or processing of sensitive personal data in a way that contradicts the law is unlawful,
- Under Article 61, providing false information during and after the registration to the supervisory authority amounts to an offence.

An offence is committed when a corporate entity or legal body violates any of the offences outlined in Articles 56, 57, 58, 59, 60, and 61. Upon conviction, the entity is liable to a fine of Rwandan francs amounting to five percent (5%) of its annual turnover of the previous financial year.

28. General Provisions

- This Policy applies to all personal data processed by **AFR**.
- The DPO shall take responsibility for **AFR**'s ongoing compliance with this policy.
- **AFR** shall maintain valid registration with the data protection officer as an organisation that processes personal data.

29. Review of this Policy

The COO is responsible for ensuring that this policy is reviewed on a timely basis. This policy will be reviewed after every five years and when necessary and accordingly approved by the Board.

30. Related Policies

The procedures and agreements that detail the measures and controls that we take to protect personal information and to ensure its security from collection to disposal are:

- Employee Privacy Notice
- Recruitment Privacy Notice
- Data Subject Rights Request Procedure
- Record Management Procedure
- Vendor Management Procedure
- Data Breach Response Plan
- Controller – Processor Agreement
- Data Sharing agreement
- Cross-border agreement

31. Changes to this Policy

This Policy may be updated to reflect best practices, legal, or regulatory changes. The latest version will be available on **AFR**'s website, and will be reviewed periodically.

Appendix:

References to related policies

This policy should be read in conjunction with:

Record Management Procedure	Privacy Notices	Website Privacy Notice
Employee Privacy Notice	Recruitment Privacy Notice	Record Owner Responsibility Undertaking
Data Subject Rights Request Procedure	Cookie Notice	CCTV Procedure
Data Breach Response Plan	Vendor Management Procedure	IT Policies and Procedures Manual

Consent Forms:

- Use of my biometric data
- Use of my personal data for business and corporate use
- Employment reference checks
- Use of my personal data for business and corporate use (Employees)

Templates:

- International Data Transfer Agreement
- Controller to Controller Contract
- Controller to Processor Contract
- Processor to Processor Contract
- Processor to Controller Contract

Signed on behalf of the Board by	
David Ferrand	Chairperson, AFR Board of Directors
Peace Uwase Masozera	Chairperson - Finance, Audit and Risk Committee

Access to Finance Rwanda

Golden Plaza – Kacyiru 3rd Floor 1 KG 546 ST
P.O BOX 1599 Kigali

Phone: +250 782 507 751
Email: info@afr.rw
www.afr.rw