ACCESS TO FINANCE RWANDA

AFR
Data Protection Policy

ACCESS TO FINANCE RWANDA

Data Protection Policy

Date of revision	July 2021
Policy owner	Chief Operating Officer (COO)
Status	Public

Versions	Description of Change implemented	Submitted by	Reviewed by the Nominating and Governance Committee on	Approved by the Board on
Version 1	New Policy	COO	12th Aug 2021	28th October 2021

List of contents

1. Introduction

Recent concerns about the security of personal data stored in institutions have led to Governments enacting data protection regulations. In 2018, the European Union (EU) operationalised the General Data Protection Regulations (GDPR) that govern how companies handle personal data. Consequently, on 13th October 2021, the Rwandan Government approved the law No 058/2021 of 13/10/2021 relating to the protection of personal data and privacy.

The law will regulate the obligations of data controllers and processors, as well as afford data subjects general rights that protect their personal information. This includes embedding principles of lawful processing, minimising the collection of data, ensuring the accuracy of data and adopting security safeguards to protect personal data.

In addition to this Law, other laws and regulations contain ancillary provisions concerning the protection of personal data:

- Information and Communication Technologies Law No. 24/2016: promulgated in 2016 in order to regulate electronic communications, information society, the broadcasting sector, and the postal sector.
- Law No. 18/2010 of 12/05/2010 relating to Electronic Messages, Electronic Signatures and Electronic Transactions: promulgated in 2010 to regulate the electronic collection of personal information.
- Furthermore, The National Bank of Rwanda has issued Regulation No. 02/2018 of 24/01/2018 (Official Gazette No. 6bis of 05/02/2018) ('the Regulation on Cybersecurity'). This Regulation aims to establish minimum standards for banks to protect against cybersecurity threats and promote the protection of customer information as well as the information technology systems of banks.

Rwanda has also set out a Data Revolution Policy ('the Policy') that targets to achieve specific objectives including, but not limited to, establishing standards and principles for data management, defining the framework for data creation-anonymisation-release, foster data-enabled technology innovations, establish data institutional governance framework, and address concerns of security-privacy and data sovereignty. The Policy requires that all current legislation and rules be checked and revised to ensure that the recommended implementation practices and data security and privacy issues are legally ensured.

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 that it protects the rights of data subjects and that the data it collects, and processes is done in line with the required legislation. AFR staff must comply with this policy, breach of which could result in disciplinary action.

3. Purpose

The policy provides guidance on how AFR will handle the data it collects. It helps AFR comply with the data protection law, protect the rights of the data subjects and protects AFR from risks related to breaches of data protection.

4. Scope

The policy applies to:

1. Employees of AFR and all AFR's associated parties such as members of the Investment Committee, implementing partners, vendors, contractors and any other third party 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;
2. All personal data processing AFR carries out for others (where AFR is the 'Processor' for the personal data being processed) and,
3. All formats, e.g., printed and digital information, text and images, documents and records, data and audio recordings.

5. Definitions

Data controller means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of the processing of personal data.

Data processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

Data subject means an identified or identifiable natural person who is the subject of personal data.

Personal data means any information relating to an identified or identifiable natural person

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed

Sensitive personal data means data that reveals the natural person's race, health status, ethnic, social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses' sex, or the sexual orientation of the data subject.

Processing data means any operation or sets of operations performed on personal data whether or not by automated means, such as (a) collection, recording, organisation, structuring; (b) storage, adaptation or alteration; (c) retrieval, consultation or use; (d) disclosure by transmission, dissemination, or otherwise making available; or (e) alignment or combination, restriction, erasure or destruction.

6. Principles

AFR will ensure that data is:

1. Processed lawfully, fairly and in a transparent manner and in line with the right to privacy.
2. Collected only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with that purpose.
3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is to be processed.
4. Accurate and where necessary kept up to date.
5. Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed.
6. Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and accidental loss, destruction, or damage.
7. Not transferred out of Rwanda unless there is proof of adequate data safeguards/ measures or consent from the data subject (after having been informed of the possible risks of the transfer owing to the absence of appropriate safeguards) and authorisation granted by the authority in charge of data protection.

7. Data protection officer

AFR has designated the Chief Operating Officer to be the Data Protection Officer (DPO). Accordingly, the DPO will:

1. Advise AFR staff on requirements for data protection, including data protection impact assessments.
2. Ensure that the AFR has complied with the legal requirements on data protection.
3. Facilitate capacity building of staff involved in data processing operations.
4. Cooperate with external regulators on matters relating to data protection.

AFR's DPO can be contacted via the email: dataprotection@afr.rw

8. 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:

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

9. Lawful and fair processing of data

AFR will only process data where they have a lawful basis to do so. Processing personal data will only be lawful where the data subject has given their consent for one or more specific purposes or where the processing is deemed necessary:

1. For the performance of a contract to which the data subject is a party (for instance a contract of employment).
2. To comply with the AFR's legal obligations.
3. To perform tasks carried out in the public interest or the exercise of official authority.
4. To protect the vital interests of the data subject or another person.
5. To pursue AFR's legitimate interests where those interests are not outweighed by the interests and rights of data subjects.
6. For historical, statistical, journalistic, literature and art or scientific research.

10. Minimisation of collection

AFR will not process any personal data for a purpose for which it did not obtain consent. Should such a need arise, then consent must be obtained from the data subject.

AFR will collect and process data that is adequate, relevant, and limited to what is necessary. 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.

Staff must ensure that they delete, destroy, or anonymise any personal data that is no longer needed for the specific purpose for which they were collected.

11. Accuracy of data

AFR must ensure that the personal data it collects and processes is accurate, kept up to date, corrected or deleted without delay. All relevant records must be updated should staff be notified of inaccuracies. Inaccurate or out of date records must be deleted or destroyed.

12. Safeguards and security of data

AFR has instituted data security measures which are laid out in the Information security policy and procedures. These measures serve to safeguard personal data and must be complied with accordingly.

13. Consent

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.

14. 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 Safeguarding policy.

AFR will institute adequate mechanisms to verify the age and obtain consent before processing the data.

15. Data protection impact assessment

AFR will undertake a data protection impact assessment whenever they identify that the processing operation will likely result in a high risk to the rights and freedoms of any data subject. The data protection impact assessment will be done before processing the data. It is the responsibility of the DPO to carry out the impact assessment.

16. Processing sensitive personal data

AFR will process sensitive personal data only when:

1. The processing is carried out in the course of legitimate activities with appropriate safeguards and that the processing relates solely to the staff or to persons who have regular contact with AFR, and the personal data is not disclosed outside that AFR without the consent of the data subject.
2. The processing relates to personal data that has been made public by the data subject.
3. Processing is necessary for:
    - The establishment, exercise or defence of a legal claim.
    - The purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject.
    - Protecting the vital interests of the data subject or another person where the data subject is physically or legally incapable of giving consent.

17. Transferring personal data out of Rwanda

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

1. The authorization 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:
    - (i) 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;
    - (ii) For the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person;
    - (iii) For reasons of public interest as provided by law;
    - (iv) For the establishment, exercise or defense of a legal claim; or
    - (v) 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
    - (vi) 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 (17)(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 (17)(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.

18. Onward reporting

In line with regulatory requirements, AFR will report to the Data Protection and Privacy Authority any data breach within 24 hours of being aware as prescribed by the law.
AFR will also communicate the data breach to the data subject as soon as is practical unless the identity of the data subject cannot be established.

19. Training and awareness

AFR will train staff on the contents and implementation of this policy. Staff who join AFR will be required to go through an induction process that entails familiarisation with this policy.

AFR will ensure that the requirements of this policy form part of its agreement with its grantees, contractors and third parties who process AFR's data.

20. 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 above.

Grantees and partners must also abide by this policy and institute adequate mechanisms to safeguard the privacy of individuals data.

21. Roles and responsibilities

All staff must:

1. Read, understand and comply with the contents of this policy
2. Report suspicions of breaches promptly

All Intervention Managers must

1. Ensure staff and third parties they work with are aware of the contents of this policy
2. Conduct risk assessments, and update controls and procedures to mitigate the risk of data breaches

The Chief Executive Officer (CEO) and Chief Operations Officer (COO) are responsible for ensuring employees, Investment Committee members, consultants, vendors, and partner organisations are aware of the policy and are supported to implement and work by it, as well as creating a management culture that encourages a focus on data protection.

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.

22. 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.

23. Data retention

The Data retention period in AFR is determined by legitimate needs. Adequate records of decision making will be maintained to show cause.

24. 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.

25. Related policies

This policy should be read in conjunction with:

1. Code of conduct
2. Misconduct, disciplinary and grievance policy
3. Information security policy

Access to Finance Rwanda

Access to Finance Rwanda
KG 5 Avenue, House No.13 Kacyiru
P.O BOX 1599 Kigali

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