AFARD

The Quest to a Better Society

FINANCE, ADMINISTRATION, AUDIT AND RESOURCE MOBILIZATION (FAARM) COMMITTEE

DATA PROTECTION POLICY

JUNE 2023

FINANCE, ADMINISTRATION, AUDIT AND RESOURCE MOBILIZATION (FAARM) COMMITTEE

DATA PROTECTION POLICY

Approved by:
Biannual Board of Directors' Meeting

JUNE 12, 2023

TABLE OF

CONTENTS

01
PURPOSE

In pursuit of its mandates, AFARD obtains, uses, stores and otherwise processes information that are linked to living individuals known as 'personal data or data subject'. Such personal data includes information about prospective, current and former staff and volunteers/interns, suppliers, project beneficiaries, website users and other contacts. This data processing may also include the need to share personal data with implementing partner or third parties as well as inherent risks such as accidental or unauthorized loss or disclosure. The purpose of this policy is to ensure that AFARD processes and protects personal data in accordance with its responsibilities under the Data Protection and Privacy Regulation 2021 and compliance with this policy is mandatory for all AFARD personnel and third parties.

TERMS AND DEFINITIONS

For the purposes of this Policy, the following definitions apply:

CONSENTS: Any freely given and informed indication of an agreement by the data subject to the processing of his/her personal data, which may be given either by a written or oral statement or by a clear affirmative action.

DATA CONTROL: The AFARD staff member who has the authority to oversee the management of, and to determine the purposes for, the processing of personal data.

DATA PROCESSOR: Any AFARD staff or other natural person or organization, including implementing partner or third party that carries out processing of personal data on behalf of AFARD.

DATA PROTECTION FOCAL POINT: In principle, the Board Secretary who assists the data controller in carrying out his or her responsibilities regarding this Policy.

DATA PROTECTION IMPACT ASSESSMENT: A process for assessing the protection impacts on data subjects in processing their personal data and for identifying remedial actions as necessary in order to avoid or minimize such impacts.

DATA PROTECTION OFFICER: The AFARD staff, in essence a manager, who supervises, monitors and reports on compliance with this Policy.

DATA SUBJECT: An individual whose personal data is subject to processing.

DATA TRANSFER AGREEMENT: An agreement between AFARD and third party that states the terms and conditions of use of personal data, including which data components are to be shared, the mode of transfer, how the data may be used, data security measures and other related issues.

IMPLEMENTING PARTNER: An organization established as an autonomous and independent entity from AFARD that AFARD engages through a project partnership agreement to undertake the implementation of programmatic activities within its mandate.

PERSONAL DATA: Any data related to an individual who can be identified from that data; other information; or by means reasonably likely to be used related to that data. Personal data includes biographical data (biodata) such as name, sex, marital status, date and place of birth, country of origin, individual registration number, occupation, religion and ethnicity, biometric data such as a photograph, fingerprint, facial or iris image.

PERSONAL DATA BREACH: A breach of data security leading to the accidental or unlawful/ illegitimate destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transferred, stored or otherwise processed.

PROCESSING OF PERSONAL DATA: Any operation, or set of operations, automated or not, which is performed on personal data, including but not limited to the collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, transfer (whether in computerized, oral or written form), dissemination or otherwise making available, correction, or destruction.

THIRD PARTY: Any natural or legal person other than the data subject, AFARD or an Implementing Partner. Examples of third parties are national governments, international governmental or non-governmental organizations, private sector entities or individuals.

02
BASIC PRINCIPLES

2.1 BASIC PRINCIPLES OF PERSONAL DATA PROCESSING

When AFARD personnel process personal data they must abide by the principles which demand that personal data is:

1. processed lawfully, fairly and in a transparent manner ('fairness and transparency').
   The 'lawfuness' requirement means that our processing of personal data must meet one of the following conditions:
   - The data subject has given consent.
   - The processing is required due to a contract.
   - It is necessary due to a legal obligation.
   - It is necessary to protect someone's vital interests (i.e. life or death situation).
   - It is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
   - It is necessary for the legitimate interests of the controller or a third party.

Special categories of personal data are restricted by extra safeguards to give further protection to the privacy of data subjects. These categories cover information relating to an individual's:

a) racial or ethnic origin
b) political opinions
c) religious beliefs or other beliefs of a similar nature
d) trade union membership
e) physical or mental health or condition
f) sex life and sexual orientation
g) generic data and biometric data

2. collected for specified, explicit and legitimate purposes; ('purpose limitation');
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization or proportionality');
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
5. safeguard the rights and freedoms of individuals ('respects the rights of data subjects'). Data subjects have the right to a copy of the information which AFARD hold about them, including the source of that information and any uses we make of it . A request can be made in writing or verbally and we must respond within one month. Whilst these requests are rare, they can legally be made to any member of staff and therefore we must ensure that all staff are aware of their responsibility to pass the details on to AFARD the same day. A written record should be kept of any verbal requests.

6. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed and in addition personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organizational measures. Appropriate back-up and recovery systems must be put in place. ('storage limitation or security');
7. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality');
8. collected, processed and protected in a manner that can be evaluated to ensure compliance with the law (Accountability and supervision).

03

RIGHTS OF THE DATA SUBJECT

3.1 INFORMATION

When collecting personal data from a data subject, AFARD should inform the data subject of the following, in writing or orally, and in a manner and language that is understandable to the data subject:

a) Who is collecting the data – AFARD directly or implementing partner or third party
b) The specific purpose(s) for which the personal data will be processed;
c) Whether such data will be transferred to Implementing Partner(s) or third parties
d) The importance of the data subject providing accurate and complete information;
e) Any consequences for refusing or failing to provide the requested and correct personal data;
f) The data subject's right to request access to their personal data, or correction or deletion of it;
g) The data subject's right to object to the collection of personal data;
h) How to lodge a complaint with the Data Protection Officer.

3.2 ACCESS

Requests for information about access to, correction or deletion of personal data or an objection, may be made by the data subject or his or her authorized legal representative, or, in the case of a child, a parent or legal guardian.

Requests are to be submitted orally or in writing to the AFARD office in the country where the data is being processed.

Upon request the data subject may receive from AFARD:

a) Confirmation as to whether or not data related to him or her has been, is being or will be processed; and
b) Information on the personal data being processed, the purpose(s) for processing such data and the Implementing Partner(s) and/or third parties to whom such data has been, is being or will be transferred.

3.3 CORRECTION AND DELETION

a) The data subject may request the correction or deletion of personal data that is inaccurate, incomplete, unnecessary or excessive.
b) Where a data subject requests the correction or deletion of his or her personal data, AFARD is to request proof relating to the inaccuracy or incompleteness.

3.4 OBJECTION

A data subject may object to the processing of his or her personal data where there are legitimate grounds related to his or her specific personal situation. If the objection is justified, AFARD should no longer process the personal data concerned.

3.5 RECORDING AND RESPONSE

a) Before complying with any request (3.3) or objection (3.4), AFARD should satisfy itself of the identity of the person making the request or objection. The individual is required to identify him or herself in an appropriate manner. In the case of a legal representative or legal guardian, proof of such legal authority needs to be supplied. Requests and objections from parents or guardians for children should be evaluated against the best interests of the child.

b) AFARD is to record the requests received for access, correction, deletion or objection and the response provided in relation to such requests.

c) AFARD is to respond to a request or objection within a reasonable time, in writing or orally, and in a manner and language that is understandable to the data subject and/or his or her legal representative or legal guardian, as applicable.

3.6 RESTRICTIONS

Based on consultations with the Data Protection Officer, AFARD may refuse to provide a response or limit or restrict its response to a request or objection where:

a) It would constitute a necessary and proportionate measure to safeguard the mandates and safety and security of personnel of AFARD or Implementing Partners.

b) There are grounds for believing that the request is manifestly abusive, fraudulent or obstructive to the purpose of processing.

04
DATA PROCESSING

4.1 CONFIDENTIALITY OF PERSONAL DATA

Personal data is by definition confidential. In order to ensure and respect confidentiality, personal data must be filed and stored in a way that it is accessible only to authorized personnel and transferred only through the use of protected means of communication.

4.2 SECURITY OF PERSONAL DATA

AFARD's data security measures are to protect personal data against the risk of accidental or unlawful/illegitimate destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. To do so:

a) AFARD will conduct staff training in data protection and security; and data protection impact assessments
b) AFARD will maintain physical security of premises, portable equipment, individual case files and records as well as computer and information technology (IT) security, for example, access control (e.g. passwords), user control, storage control, input control, communication and transport control (e.g., encryption).

4.3 ENSURING ACCURACY OF PERSONAL DATA

a) AFARD may correct or delete personal data held on its systems that is inaccurate, incomplete, unnecessary or excessive.
b) When personal data is corrected or deleted in AFARD's systems, AFARD should notify, as soon as reasonably practicable, all Implementing Partners and/or third parties to whom the relevant personal data was transferred.

4.4 NOTIFICATION OF A PERSONAL DATA BREACH

a) Personal data breaches could occur through: Loss or theft of data or equipment; Ineffective access controls allowing unauthorized use; Equipment failure; Unauthorized disclosure (e.g. email sent to the incorrect recipient); Human error; and hacking attack.

b) Upon becoming aware of a personal data breach, AFARD personnel are required to notify the data controller as soon as possible and to properly record the breach. The notification should describe:
   i. The nature of the personal data breach, including the categories and number of data subjects and data records concerned;
   ii. The known and foreseeable adverse consequences of the personal data breach; and

iii. The measures taken or proposed to be taken to mitigate and address the possible adverse impacts of the personal data breach.

c) In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, AFARD will promptly assess the risk to people's rights and freedoms and if appropriate report this breach within the required deadline.

d) If a personal data breach is likely to result in personal injury or harm to a data subject, the data controller should use his or her best efforts to communicate the personal data breach to the data subject and take mitigating measures as appropriate without undue delay. In such cases, the data controller should also notify the Data Protection Officer of the personal data breach.

4.5 DATA PROTECTION IMPACT ASSESSMENTS

a) When elaborating new systems, projects or policies or before entering into data transfer arrangements with Implementing Partners or third parties which may negatively impact on the protection of personal data of persons of concern, AFARD needs to carry out a Data Protection Impact Assessment (DPIA). A DPIA is required where the collection and processing or transfer of personal data is likely to be large, repeated or structural (i.e. where data is shared with an Implementing Partner or third party over a certain period of time).

b) A DPIA would contain a general description of the envisaged system, project, policy or data sharing arrangement involving processing of personal data, an analysis of the risks to the rights of data subjects by virtue of the circumstances and the nature of the personal data processed, the safeguards, security and other measures in place or proposed to ensure the compliance with this Policy.

c) Data controllers are responsible for organising and carrying out DPIAs, when required. DPIAs are normally carried out at the country level unless it is decided that a DPIA is to be carried out at global or regional level due to the scope of system or arrangement.

d) Data controllers are to keep the Data Protection Officer fully informed of any DPIA carried out under their responsibility and to share a copy of the DPIA.

4.6 RETENTION

a) Personal data that is not recorded in individual case files is not to be retained longer than necessary for the purpose(s) for which it was collected.

b) All individual case files, whether open or closed, are considered permanent records, and must therefore be permanently retained in line with the Access Policy of AFARD Archives

05

DATA PROCESSING BY PARTNERS

5.1 GENERAL CONDITION

Where the collection and processing of personal data is one of the responsibilities of Implementing Partners, the personal data is being collected and processed on behalf of AFARD. For these reasons, Implementing Partners are expected to respect and implement the same or comparable standards and basic principles of personal data protection as contained in this Policy.

5.2 VERIFICATION

AFARD will verify that the processing of personal data by the Implementing Partner satisfies the standards and basic principles of this Policy. Such verification may form part of a Data Protection Impact Assessment.

5.3 PARTNERSHIP AGREEMENTS

To ensure compliance, AFARD will include in its partnership agreements with Implementing Partners clauses that specifically requires compliance with personal data protection.

5.4 CAPACITY OF THE PARTNER

AFARD will assist Implementing Partners in building or enhancing their capacity to comply with the data protection standards and principles contained in this Policy. Such assistance may relate to the establishment of policies, the delivery of training or putting in place technical and organizational measures.

5.5 PARTNERSHIP TERMINATION

AFARD will ensure that after termination of a partnership with assist Implementing Partners , all personal data collected in the performance of the partnership are returned to AFARD except where there are legitimate reasons to do so, namely consent of the data subjects.

06

TRANSFER OF PERSONAL DATA

6.1 GENERAL CONDITIONS

6.1.1 AFARD may transfer personal data to third parties on condition that the third party guarantees compliance with this policy.

6.1.2 Given the potential data protection risks involved in transfers to third parties, AFARD will ensure that the Data Protection Officer conducts Data Protection Impact Assessment to ascertain that:

a) Transfer is based on legitimate reasons;
b) Transfer is for specific and legitimate purposes;
c) The personal data to be transferred is adequate, relevant, necessary;
d) The data subject has been informed about the transfer of his/her personal data;
e) The third party has the organizational and technical capacity to respect the confidentiality of transferred personal data .
f) Personal data is transferred strictly to authorized personnel and only through the use of protected means of communication;
g) The third party maintains a high level of data security that protects personal data against the personal data breach.
h) Transferring personal data does not negatively impact the safety and security of AFARD personnel and/or personnel of Implementing Partners; and/or the effective functioning of an AFARD operation or compromise AFARD's mandate, for example due to the loss of the climate of trust and confidence between AFARD and persons of concern or the loss of the perception of AFARD as an independent, humanitarian and non-political Organization.

6.2 DATA TRANSFER AGREEMENTS

Unless there are satisfactory reasons not to do so, AFARD will sign a data transfer agreement prior to transferring personal data to a third party. This will detail the data transfer purpose, specific data elements, data protection and data security requirements and supervision, accountability and review mechanisms for the oversight of the transfer for the life of the agreement.

07

ACCOUNTABILITY AND SUPERVISION

7.1 ACCOUNTABILIY AND SUPERVISION STRUCTURE

AFARD's accountability and supervision structure will consist of the following key actors:

a) A Data Protection Officer who is the Board Secretary.
b) Data controllers who are the Directors of Programmes and Finance and Administration, and
c) Data Protection Focal Points who are the Project Managers and Human Resource Officer and Accountants.

7.2 DATA CONTROLLER AND DATA PROTECTION FOCAL POINT

The data controllers are responsible for establishing and overseeing the processing of personal data. Given the day-to-day personal data processing in AFARD's mandate, the data controller will work hand in hand with data protection focal points to bear the main responsibility for compliance with this policy. Where necessary, they should seek the advice of the Data Protection Officer concerning queries with regard to the application and interpretation of this policy.

7.3 DATA PROTECTION OFFICER

AFARD will appoint a Data Protection Officer whose tasks will include:

a) Providing advice, support and training on data protection and this policy;
b) Maintaining inventories of information provided by data controllers and data protection focal points, including data transfer agreements, data protection impact assessments, data breach notifications and complaints by data subjects;
c) Ensuring data controllers and other relevant actors to undertake measures aimed at compliance with this policy;
d) Monitoring and reporting on compliance with this policy;
e) Submitting annual data protection report to the National Data Protection Office; and
f) Renewal of AFARD certificate of registration with National Data Protection Office.