DATA PROTECTION POLICY[1]

August 2020

[1] This is a living document whose contents may be modified or deleted at any time by AGRA at its sole discretion.

Table of Contents

1. **Policy Statement** 3
2. **Definitions** 3
3. **Scope** 5
4. **Policy Framework** 7
5. **Personal Data Protection Principles** 7
6. **Data Subject Rights** 8
7. **Lawful Processing and Consent** 9
8. **Responsibilities** 12
9. **Data Sharing** 15
10. **Data Protection Breaches** 16
11. **Impact Assessments / Risk Assessments** 17
12. **Procurement** 17
13. **Security of Electronic Data** 18
14. **Retention and Disposal of Data** 18
15. **Routine Publication of Information** 19
16. **Compliance** 19
17. **Privacy Complaints or Breaches** 20

AGRA Data Protection Policy

1. Policy Statement

1.1. AGRA and its governing body, the Board of Directors, are committed to promoting and maintaining good corporate governance. This Policy is intended to facilitate the protection of Personal Data by complying with Regulatory Requirements on Personal Data protection.

1.2. AGRA is committed to protecting the rights and freedoms of Data Subjects and safely and securely processing their data in accordance with all of applicable legal obligations. AGRA holds Personal Data about our employees, Partners, Board of Directors, for a variety of purposes as detailed in clause 3.3 of this Policy.

2. Definitions

For the purpose of this Policy, the following definitions shall apply:

"Anonymize" means to Process Personal Data with the aim of irreversibly preventing the identification of the Data Subject to whom it relates by rendering it anonymous in such a manner that the Data Subject is not or no longer identifiable.

"Consent" means that the Data Subject or as appropriate parent or the legal guardian has been fully informed of the clear intended processing and has signified their agreement, while being in a fit state of mind to do so and without pressure being exerted upon them. The Data Subject, parent, or legal guardian, as the case may be, must give Consent freely of his or her own accord.

"**Data Controller**" refers to the Natural Person or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

"Data Processor" refers to a Natural Person or legal person, public authority, agency or other bodies that process Personal Data on behalf of the Data Controller.

"Data Protection Advisory Committee" refers to an advisory committee comprising of the General Counsel, The Head of the Information and Communications Technology, the Director of Human Resources and Administration and the Head of the Monitoring and Evaluation functions.

"Data Protection Officer" for the purpose of this Policy, the Data Protection Officer is the General Counsel.

"Data Subject" refers to any Natural Person who is the subject of Personal Data Processed or held within AGRA systems.

"Regulatory Requirements" refer to all relevant national and international laws on data protection applicable to AGRA's operations that shall be in force at the time.

"Natural Person" refers to an individual human being, as opposed to an organization.

"Partners" means grantees, consultants, suppliers, any parties we have a contractual relationship with and their respective subcontractors.

"Personal Data" means any information that relates to a Natural Person from which that person can be identified. This includes but is not limited to name as well as other identifiers such as unique personal identifiers (e.g. national identification number, passport number, payroll numbers), address, location data or other online identifiers, as well as physical, physiological, genetic, mental, economic, cultural or social identity.

"Pseudonymize" refers to the Processing of Personal Data in such a way that the data can no longer be attributed to a specific Data Subject without the use

of additional information by exchanging Personal Data with non-identifying data.

"**Process"** is defined very broadly and encompasses any action performed on or with Personal Data including collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction (that is, the marking of stored data with the aim of limiting its processing in the future), erasure and destruction.

"Sensitive Personal Data" means Personal Data that reveals a Data Subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric and health data, and information relating to a Data Subject's sex life or sexual orientation.

"Third Party" means any individual/organisation other than the Data Subject, AGRA or Partners.

3. Scope

3.1. This Policy applies to all prospective, current and former employees, Partners, and all users of data held in AGRA's systems. In addition, AGRA's Partners, Board of Directors, temporary employees, interns and those undertaking work experience at AGRA are required to observe the data protection principles and to comply with the responsibilities set out in this Policy.

3.2. AGRA may supplement or amend this Policy by effecting guidelines and tools from time to time that shall be circulated to the persons covered by this Policy. This Policy shall be reviewed regularly but at the very least every two years.

3.3. AGRA Processes Personal Data for various purposes, including human resource, administrative, financial, regulatory, payroll and business development purposes, among others. These specific areas covered include (but are not limited to) the following:

a) Compliance with our donor, legal, regulatory and corporate governance obligations and good practices.
b) Provision of information to our donors when and to the extent necessary for the purposes of the legitimate interest pursued (such as seeking to ensure that the donors are working with appropriately qualified individuals).
c) Gathering of information as part of investigations by regulatory bodies or in connection with legal proceedings or requests.
d) Ensuring AGRA policies are adhered to (such as policies covering the use of AGRA's information systems and resources, such as email and internet).
e) Operational reasons such as recording transactions, training and quality control, and ensuring the confidentiality of sensitive information.
f) Investigating complaints.
g) Checking references, ensuring safe working practices, monitoring and managing employee access to systems and facilities and employee absences, administration and assessments.
h) Monitoring employee conduct and disciplinary matters.
i) Monitoring the utilization of AGRA's information technology resources.
j) Marketing our work.
k) Improving services.
l) Maintenance of employees' and stakeholders' information that is useful for the delivery of AGRA's strategy.
m) Maintenance of complete and meaningful information repositories for organizational and stakeholder use.
n) Accountability, transparency and responsible use of AGRA's resources.
o) Cybersecurity surveillance.

4. Policy Framework

4.1. AGRA's Personal Data protection and privacy requirements are captured across various institutional policies and procedures. This Policy shall be used in conjunction with, referenced to and shall be referenced by other AGRA policies including but not limited to the following:

a) Anti-Money Laundering Policy;
b) Disciplinary Policy & Procedures;
c) Ethics Policy;
d) Human Resources Policies;
e) ICT Policies and Procedures;
f) Partners Code of Conduct;
g) Policy on the Management of Intellectual Property Assets; and
h) Safeguarding of Vulnerable Persons Policy.

4.2. We interpret our policies taking into consideration the spirit of this Policy and shall appropriately apply the Data Protection principles in interpreting data protection issues under each of the other AGRA policies.

5. Personal Data Protection Principles

5.1. AGRA commits to comply with the following principles when Processing Personal Data. Personal Data shall be:

a) processed lawfully, fairly and in a transparent manner.
b) collected for specified, clear and legitimate purposes and not Processed for other purposes other than those specified.
c) processed adequately for the requirement, relevant and limited to what is necessary in relation to the purposes for which they are processed.
d) accurate and, as necessary, kept up-to-date.
e) retained for the minimum period required to meet AGRA's Regulatory Requirements for the successful undertaking of AGRA's business objectives.

f) in a manner that ensures its security, including protection against unauthorised or unlawful access and against accidental loss, destruction or damage.
g) transferred only where there is adequate protection for the Personal Data.
h) handled in respect of owners' intellectual property rights and informed consent requirements.

5.2. AGRA shall inform Data Subjects of the reasons for Processing their Personal Data, how it uses such Personal Data, the legal basis for Processing and where required seek Consent from the Data Subject. It shall not process Personal Data of Data Subjects for other incompatible reasons.

5.3. Sensitive Personal Data shall be Processed with strict controls as set out in clause 7.4 of this Policy and within available technological constraints.

6. Data Subject Rights

6.1. AGRA respects the rights of Data Subjects to access the Personal Data that AGRA processes about them.

6.2. Data Subjects have specific rights regarding the Processing of Personal Data Processed by AGRA:
a) Right to information on what the Personal Data shall be used for.
b) Right of access to Personal Data where such access does not violate the privacy of other Data Subjects' Personal Data.
c) Right to objection to processing of all Personal Data or part of the Personal Data.
d) Right to erasure of false or misleading Personal Data.
e) Right to correction of false or misleading Personal Data.

6.3. **Rights in relation to automated decision making and profiling**

The Data Subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

AGRA must respect the rights of Natural Persons in relation to automated decision making and profiling and can only carry out such type of decision-making or profiling where the decision or profile is:

a) necessary for the entry into or performance of a contract;
b) authorised by Regulatory Requirements;
c) based on the Data Subject's informed Consent;
d) necessary for the assurance of the security of AGRA's information assets;
e) required for successful delivery of AGRA's strategy; or
f) for the benefit of the Data Subject without possible harm.

7. Lawful Processing and Consent

7.1. All Processing undertaken by AGRA must be lawful. It is only lawful to undertake the Processing of Personal Data where the Processing is in accordance with Regulatory Requirements and on the following basis:

a) With the informed Consent of the Data Subject;
b) Processing is necessary for the performance of a contract with the Data Subject or to take steps to enter into a contract;
c) Processing is necessary for compliance with a legal obligation;
d) Processing is necessary to protect the vital interests of a Data Subject or another person;
e) Processing is necessary to protect the confidentiality, integrity and availability of AGRA's information assets.
f) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller; or

g) Necessary for the purposes of legitimate interests pursued by the Data Controller or a Third Party, except where such interests are overridden by the interests, rights or freedoms of the Data Subject.

7.2. Where another basis for Processing Personal Data does not exist, Personal Data or Sensitive Personal Data can only be Processed with the informed Consent of the Data Subject.

7.3. Consent can be provided in a range of forms including verbal, electronic and written Consent. All Consent must require a positive selection or choice to opt in. Where verbal Consent is obtained then records of the Consent must be maintained.

7.4. For Sensitive Personal Data, clear written Consent of Data Subjects must be obtained unless an alternative lawful basis for processing exists. In addition, Sensitive Personal Data shall be processed where the following conditions exist:

a) If the Data Subject has given Consent to the processing of Sensitive Personal Data for one or more specified purposes (the Personal Data may be processed, but only for the purpose approved by the Data Subject).
b) If the Data Subject is physically or legally incapable of giving a Consent and the processing is necessary to protect the vital interests of the Data Subject or any other Natural Person.
c) Where the processing of the Sensitive Personal Data is necessary to carry out obligations and exercising specific rights of AGRA as a Data Controller or for the exercising of specific rights of a Data Subject.
d) Where the processing of Sensitive Data is necessary for AGRA to establish, exercise or defend a legal claim.

e) When the Data Subject manifestly has made the Sensitive Personal Data public,
f) Where the exceptions are contained in supplementary data protection regulations.
g) In the field of labor law, social security and social protection necessary for AGRA to fulfil its obligations and rights as an employer.
h) Where the processing of the Sensitive Personal Data is necessary for an important public interest.
i) For archiving purposes or research purposes where AGRA is obligated to archive documents for the need for administrative procedure and for research needs. Sensitive Personal Data may be processed if it is necessary to comply with such archiving purposes. If the sole purpose of processing Sensitive Personal Data is archiving, then that data may not be used for other purposes, unless there are particular reasons to do so with regard to the Data Subject's vital interests. However, this use limitation does not apply to Personal Data contained in public documents.
j) For statistical purposes where the processing of Sensitive Personal Data is in the public interest which clearly outweighs the risk of intrusion to the privacy of the Data Subject.
k) Where it is deemed necessary for investigations relating to electronic fraud or related unauthorized systems access or any other actions that are in violation of AGRA's ICT policies.

7.5. In most instances AGRA shall process Personal Data on a legal basis other than Consent. Where Consent is used as the legal basis of Processing then Consent shall be obtained before any processing is undertaken. Any AGRA forms (whether electronic or paper-based) that gather Personal Data on an individual should contain a statement explaining what the information is to be used for and to whom the information that is may be disclosed. Separate Consent is required for each separate processing

activity and usage of the Personal Data where Consent is used as the legal basis of processing. If an individual does not consent to certain types of Processing, appropriate action must be taken to ensure that the Processing does not take place.

7.6. Where Consent has been obtained, it must be recorded. AGRA is responsible for recording and maintaining an up to date record of the Consent that has been obtained where it is the basis of Processing.

7.7. Consent can be withdrawn at any time. If Consent is withdrawn, then any Personal Data held on the basis of that Consent should be removed from AGRA records subject to the applicable Regulatory Requirements for retaining such information.

7.8. AGRA Reserves the right to disclose Personal Data if the Data Subject is involved in any form of electronic fraud and/or cyber espionage.

8. Responsibilities

8.1. **AGRA's responsibilities**

8.1.1. AGRA is a Data Controller and/or Data Processor under the data privacy regulations. Where AGRA engages a Third Party to process Personal Data (such as payroll), an agreement that is compliant with Regulatory Requirements shall be set up with the supplier/service provider. AGRA must require sufficient guarantees under data privacy laws from Data Processors including sufficient guarantees that the rights of Data Subjects shall be respected and protected.

8.1.2. Regularly review and only retain Personal Data relevant to the purpose it was provided for.

8.1.3. Documenting the type of Personal Data AGRA Processes, the Processing purposes and the lawful basis for Processing.

8.1.4. Comply with data protection principles as detailed in clause 5 of this Policy.

8.1.5. Enable the Data Subjects to exercise their rights as described in clause 6 of this Policy.

8.1.6. Ensure AGRA's employees receive appropriate training on data protection requirements.

8.1.7. Implementing and reviewing procedures to detect, report and investigate Personal Data breaches.

8.1.8. Store Personal Data in safe and secure ways.

8.1.9. Assess the risk that could be posed to individual rights and freedoms should Personal Data be compromised.

8.2. **Responsibilities of AGRA's Employees and Partners**

8.2.1. Line managers and their reports should ensure they are familiar with this Policy in the Processing of all Personal Data to which they have access to in the course of their duties.

8.2.2. Employees with access to and responsibility for Personal Data are expected to:

a) Access only Personal Data that they have authority to access and only for authorized purposes;
b) Use Personal Data responsibly and in accordance with the Data Protection Principles;
c) Exercise caution before disclosing Personal Data both within and outside AGRA, or before using it in email, through the internet or intranet;
d) Report any loss or compromise of their own or others' Personal Data to the Data Protection Officer;
e) Take all necessary action to keep Personal Data secure, no matter its form or format, including by the proper management of electronic devices, including mobile devices and computer access; implementing and complying with rules on access to AGRA premises and secure electronic and hard copy file storage and destruction, and in accordance with corporate policies and guidance.
f) Where Personal Data is to be disposed of, the Data Protection Officer should ensure that it is destroyed securely subject to retention requirements. It must be remembered that the destruction of Personal Data is of itself Processing and must be carried out in accordance with the data protection principles;
g) AGRA employees must not send other people's Personal Data from an AGRA device including laptop, desktop, tablet or mobile phone to a personal email account such as an account not owned or controlled by AGRA, except where it is legally permitted to do so;
h) Where employees' Personal Data needs to be taken off site the responsible employee must ensure that appropriate steps are taken to protect it; be it in hard copy, stored on a laptop or other electronic device. For the removal of hard copy information, prior consent should be obtained from their line manager and unit head;
i) Care must also be taken when observing Personal Data in hard copy or on-screen so that such information is not viewed by anyone who is not legitimately privy to it; and

j) If an employee is in any doubt about what they may or may not do with Personal Data, they should seek advice from the Data Protection Officer before taking any action.

k) Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this Policy or Regulatory Requirements without delay.

8.3. **Responsibility for this Policy**

8.3.1. The Data Protection Officer, who is the General Counsel for the purpose of this Policy, has overall responsibility for AGRA's Personal Data protection compliance and the day-to-day implementation of this Policy.

8.3.2. A Data Protection Advisory Committee comprising the Director of Human Resources, Head of ICT, Head of Communications and Head of Monitoring and Evaluation shall support the Data Protection Officer in this role.

9. Data Sharing

9.1. AGRA shall ensure that no Personal Data is transferred to a country or organization unless that country or organization ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of Personal Data, unless such transfer is for compliance with AGRA's data protection in accordance with AGRA's ICT Policies and AGRA's Business Continuity Plans.

9.2. AGRA shall use encryption and/or Pseudonymisation where it is appropriate to do so.

9.3. AGRA shall in some circumstances have to share Personal Data with Third Parties, including service providers and other statutory bodies. AGRA shall require Third Parties to fully comply with this Policy.

9.4. AGRA shall ensure that Personal Data held in organizational ICT resources that traverse national boundaries are shared across systems (such as websites, integrated information systems among others) in compliance with this Policy and/or applicable Regulatory Requirements.

10. Data Protection Breaches

10.1. Failure to observe the Data Protection Principles within this Policy may result in the employee and Third Parties incurring personal criminal liability. It may also result in disciplinary action up to and including dismissal of an employee where there are significant or deliberate breaches of this Policy, such as accessing Personal Data without authorization or a legitimate reason to do so.

10.2. Employees must immediately report to the Data Protection Officer and the Data Protection Advisory Committee any actual or suspected data protection breaches.

10.3. If AGRA discovers that there has been a breach of employee-related Personal Data that poses a risk to the rights and freedoms of individuals, it shall inform affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken to address the breach.

10.4. Where AGRA engages Third Parties to process personal data on its behalf, such parties do so based on written instructions, are under a duty of

confidentiality and are obliged to implement appropriate technical and organizational measures to ensure the security of data.

10.5. AGRA shall not be held responsible for disclosure of Personal Data in its possession that is also held in other public or private systems.

11. Impact Assessments / Risk Assessments

11.1. Decisions around the processing of Personal Data within AGRA shall be undertaken with suitable regard for the risk and impact to the privacy and rights of Data Subjects before processing for large volumes of Personal Data is undertaken.

11.2. Data Protection Impact Assessments will be undertaken when a new business process or processing activity is developed that involves the use of Personal Data.

12. Procurement

12.1. Data protection issues must be considered at the point of procurement where the goods or services being procured have an impact on data protection and involve the handling of Personal Data.

12.2. Before a new supplier can be involved in the processing of Personal Data held by AGRA, a contract must exist which sets out the obligations and requirements of the supplier to the processing of the Personal Data. The supplier must be subject to appropriate due diligence in regard to their data protection practices.

12.3. AGRA shall maintain a register of organisations whose data protection practices have been verified and approved and a record of the contract that is in place.

13.Security of Electronic Data

13.1. The ICT Information Security Policy sets out the requirements for the secure handling and management of electronic data and secure use of information technology systems; the policy plays a significant role in the effectiveness of Personal Data protection within AGRA. All AGRA employees and stakeholders are responsible for ensuring that they are familiar with and comply with the ICT Security Policy and other related ICT policies at all times.

13.2. Access to Personal Data should be limited to those who need to access it in undertaking their legitimate duties as part of AGRA.

14. Retention and Disposal of Data

14.1. Personal Data should not be retained longer than is required for the lawful processing of the Personal Data. Once the Personal Data is no longer required for a specific purpose then it must be disposed of in a way that protects the rights and privacy of Data Subjects or Anonymized Personal Data and maintains a trail of activity on the Personal Data for compliance purposes.

14.2. There are a range of different legal and statutory obligations requiring the retention of information that impact AGRA's activities as a Data Controller. Personal Data must be retained in accordance with all applicable Regulatory Requirements.

15. Routine Publication of Information

15.1. AGRA publishes a number of items that include Personal Data which includes but is not limited to:

a) Names of all members of the Board of Directors and management.
b) Names and job titles of employees.
c) Internal telephone directory.
d) Information in prospectuses (including photographs), brochures, annual and other reports, and newsletters.
e) Employee information on AGRA website including photographs.
f) Information about stakeholders that interact with AGRA in its day to day activities.

15.2. It is recognised that there might be occasions when a Data Subject, requests that their Personal Data in some of these categories remain confidential or are restricted to internal access. The individuals should be offered an opportunity to opt-out of the publication of the above (and other) data. In such instances, AGRA should endeavour to comply with the request where possible and ensure that appropriate action is taken. However, where the Personal Data is published for regulatory reasons or where the Personal Data is published because of a legal, compliance or security obligation then the information shall continue to be published.

16. Compliance

16.1. AGRA complies with all Regulatory Requirements. It is the responsibility of all AGRA employees and stakeholders to ensure, by taking legal advice, that they are aware of all laws, regulations and policies which may affect the area of work in which they are engaged.

16.2. Likewise, AGRA complies with obligations placed on us by our development partners. It is the responsibility of all AGRA employees to ensure that they understand and comply with requirements of Partners.

16.3. Where there is any doubt about compliance requirements related to Regulatory Requirements or obligations from Partners, further guidance should be sought from the office of the General Counsel.

17. Privacy Complaints or Breaches

17.1 If an individual wishes to access or change their personal information, or to lodge a complaint about a possible breach of privacy or has any query on how personal information is collected or handled, they should contact the Data Protection Officer if by mail through:

Office of the General Counsel

AGRA

P. O. Box 66773-00800

Waiyaki Way, Nairobi

Kenya

info@agra.org