



The Agricultural Market Development Trust

Nairobi Office

Applewood Adams | Ngong Road | Suite 808

P.O. Box 14184 – 00800 NAIROBI | **Phone:** +254.720.384.724

E-Mail: info@agmark.org | **Website:** www.agmark.org

DATA PROTECTION POLICY

September 2026

DATA PROTECTION POLICY

1. POLICY STATEMENT

AGMARK collects and processes personal data belonging to its Staff, Partners, Donors, and the smallholder farmers, agrodealers, and other programme participants (together referred to as Data Subjects) it works with across its countries of operation. AGMARK is committed to protecting the privacy of Data Subjects and to the lawful, fair, and transparent processing of their personal data.

AGMARK recognizes that the collection, storage, and use of personal data, particularly the profiling and monitoring data it gathers from agrodealers, farmers, and trainees through its baseline surveys and programme databases, carries a responsibility to safeguard that data from misuse, loss, or unauthorized disclosure. This policy sets out AGMARK's commitment to the protection of personal data and provides mandatory guidelines on how Staff and Partners must collect, process, store, and share personal data in the course of AGMARK's programmes and operations.

2. PURPOSE OF THE POLICY

The purpose of this policy is to provide clarity to all of AGMARK's Staff and Partners on:

- (i) The principles that govern how AGMARK collects, uses, stores, and shares personal data.
- (ii) The rights of Data Subjects whose personal data AGMARK processes.
- (iii) Their responsibility to report any suspected or actual personal data breach.
- (iv) How personal data may be transferred across AGMARK's countries of operation and to Donors and other third parties.

We recognize that data protection legislation may vary from country to country. This policy sets out AGMARK's minimum standards, drawing on Kenya's Data Protection Act, 2019 (the "Data Protection Act") and applicable international data protection standards, including the EU General Data Protection Regulation (GDPR), and may exceed the requirements of local legislation. The policy is applicable to all Staff and Partners wherever they live and work.

This policy shall be read and applied in conjunction with other AGMARK policies, including but not limited to the following:

- (i) Safeguarding of Vulnerable Persons and Youth Policy
- (ii) Ethics Policy
- (iii) Partners Code of Conduct
- (iv) Whistleblowing Policy
- (v) Human Resources Manual, including disciplinary policies & procedures
- (vi) Information Security Policy and procedures

3. SCOPE OF THE POLICY

This policy applies to:

- (i) all categories of Staff;
- (ii) all Partners dealing with AGMARK, including grantees, collaborators, suppliers, consultants, vendors, and sub-contractors, together with their employees, agents, and representatives. All Partners are responsible for providing their employees, representatives, agents, sub-contractors, and officials with a copy of this policy; and
- (iii) all personal data AGMARK collects, holds, or processes, whether relating to Staff, Partners, Donors, or the agrodealers, farmers, and other programme participants AGMARK works with, and in whatever format it is held, including printed and digital information, text, images, audio recordings, and data held in AGMARK's databases and data collection tools.

This policy applies whether AGMARK is the Data Controller, determining the purpose and means of processing, or a Data Processor, processing personal data on behalf of another party such as a Donor or Partner.

4. DEFINITIONS

- (i) **Beneficiary:** An agrodealer, smallholder farmer, trainee, or other individual who participates in or benefits from an AGMARK programme, and whose personal data AGMARK collects in that capacity.
- (ii) **Child:** A person who is under 18 years of age, consistent with AGMARK's Safeguarding of Vulnerable Persons and Youth Policy.
- (iii) **Consent:** Any freely given, specific, informed, and unambiguous indication of a Data Subject's wishes, given by a statement or clear affirmative action, signifying agreement to the processing of personal data relating to them.
- (iv) **Data Controller:** A natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purpose and means of processing personal data.
- (v) **Data Processor:** A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the Data Controller.
- (vi) **Data Protection Officer (DPO):** The individual designated by AGMARK to oversee compliance with this policy and applicable data protection law.
- (vii) **Data Subject:** An identified or identifiable natural person who is the subject of personal data, including Staff, Partners, Donors, and Beneficiaries.
- (viii) **Donor(s):** Any party that has made a grant to AGMARK.
- (ix) **ODPC:** The Office of the Data Protection Commissioner, Kenya's data protection regulator established under the Data Protection Act, 2019.

- (x) **Partners:** Any parties with a contractual relationship with AGMARK, as well as those sub-contracted to work in an AGMARK programme, including grantees, collaborators, suppliers, consultants, their employees, volunteers, sub-contractors, officers, agents, and representatives.
- (xi) **Personal Data:** Any information relating to an identified or identifiable natural person.
- (xii) **Personal Data Breach:** A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
- (xiii) **Processing:** Any operation or set of operations performed on personal data, whether or not by automated means, including collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, transmission, dissemination, alignment, combination, restriction, erasure, or destruction.
- (xiv) **Sensitive Personal Data:** Data revealing a natural person's race, health status, ethnic or social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details (including the names of a person's children, parents, or spouse), sex, or sexual orientation.
- (xv) **Staff:** Individuals who work for AGMARK either full-time or part-time for wages and salary.
- (xvi) **Youth:** A person above the age of 18 years and under the age of 35 years, consistent with AGMARK's Safeguarding of Vulnerable Persons and Youth Policy.

5. DATA PROTECTION PRINCIPLES

AGMARK will ensure that personal data is:

- (i) Processed lawfully, fairly, and in a transparent manner and in line with the Data Subject's right to privacy.
- (ii) Collected only for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with that purpose.
- (iii) Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- (iv) Accurate and, where necessary, kept up to date.
- (v) 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.
- (vi) Processed in a manner that ensures its security, using appropriate technical and organizational measures to protect against unauthorized or unlawful processing and against accidental loss, destruction, or damage.
- (vii) Not transferred outside a Data Subject's country without proof of adequate data protection safeguards or the consent of the Data Subject.

6. WHAT PERSONAL DATA AGMARK COLLECTS AND HOW

AGMARK's programmes require it to understand the agrodealers, smallholder farmers, and other Beneficiaries it works with, primarily through baseline surveys and profiling exercises conducted at the start of a programme and updated periodically over its life. This section describes the personal data these exercises typically collect and how AGMARK collects it.

6.1 Categories of Personal Data

Depending on the programme, AGMARK may collect the following categories of personal data from Beneficiaries, Staff, and Partners:

- (i) **Identification and contact data:** name, national identification number, sex, age or age group, telephone number(s), email address, and postal address.
- (ii) **Geographic data:** country, region, county or sub-county, market centre or town, area of operation (rural, semi-urban, or urban), and GPS coordinates of a business or farm.
- (iii) **Business and livelihood data:** business name, level of education, agricultural input and output sales records, financial services used, business records, and participation in trainings, demand creation activities, and associations.
- (iv) **Observations and feedback** recorded by AGMARK's enumerators during data collection, including comments and responses to survey questions.

AGMARK does not seek to collect Sensitive Personal Data as part of its routine programme data collection and will only do so in the limited circumstances set out at Section 11 of this policy.

6.2 How Data Is Collected

- (i) AGMARK develops its data collection tools with input from relevant stakeholders and adapts them to the requirements of each specific programme.
- (ii) Data collection is carried out either manually (paper-based) or electronically (using smart devices or digital data collection systems), and occasionally remotely, such as through telephone interviews.
- (iii) Data collection is carried out by trained data clerks and enumerators, supervised by AGMARK's Data Team, who are responsible for ensuring that data is collected accurately and in accordance with this policy.

6.3 How Data Is Used

AGMARK uses the personal data it collects to:

- (i) Build and maintain programme databases used to design, monitor, and improve AGMARK's programmes.
- (ii) Prepare reports on programme implementation and progress for Donors and other stakeholders.
- (iii) Develop targeted training materials and courses for agrodealers and other Beneficiaries.

- (iv) Share aggregate or specific data, where necessary and permitted, with relevant Government line ministries and Development Partners in furtherance of AGMARK's programmes.

AGMARK acknowledges that its programme databases have historically been programme-specific rather than centralized, and that data collection has been dependent on available funding. AGMARK is committed to progressively investing in more secure, centralized, and regularly updated data systems, consistent with the principles set out in this policy.

7. LAWFUL BASIS FOR PROCESSING PERSONAL DATA

AGMARK will only process personal data where it has a lawful basis to do so. Processing personal data will only be lawful where the Data Subject has given Consent for one or more specific purposes, or where the processing is necessary:

- (i) For the performance of a contract to which the Data Subject is a party, such as a contract of employment or a grant or partnership agreement.
- (ii) To comply with AGMARK's legal obligations.
- (iii) To protect the vital interests of the Data Subject or another person.
- (iv) For the performance of a task carried out in the public interest.
- (v) To pursue AGMARK's legitimate interests, including monitoring, evaluation, and reporting on its programmes, where those interests are not outweighed by the interests and rights of the Data Subject.
- (vi) For historical, statistical, journalistic, literary and artistic, or scientific research purposes.

8. RIGHTS OF DATA SUBJECTS

AGMARK will notify Data Subjects of their rights before processing their personal data. Every Data Subject has the right:

- (i) To be informed of the use to which their personal data is to be put, including the purpose of collection and any third parties to whom it may be disclosed.
- (ii) To access their personal data in AGMARK's custody.
- (iii) To object to the processing of all or part of their personal data.
- (iv) To the correction of false or misleading data.
- (v) To the deletion of false or misleading data about them.

Where a Data Subject is a Child, or has a mental or other disability, these rights may be exercised by their parent, guardian, or another person duly authorized to act on their behalf.

9. CONSENT

Where AGMARK relies on Consent as the basis for processing personal data, it will maintain adequate records to demonstrate that Consent was obtained before processing began. Consent must be freely given, specific, informed, and unambiguous. A Data Subject has the right to withdraw their Consent at any time, and personal data will not be processed further after Consent has been withdrawn, save where another lawful basis for processing applies. The withdrawal of Consent does not affect the lawfulness of processing carried out before it was withdrawn.

10. PROCESSING PERSONAL DATA OF A CHILD

AGMARK will not process personal data relating to a Child unless Consent is given by the Child's parent or guardian, and the processing is carried out in a manner that protects and advances the rights and best interests of the Child, consistent with AGMARK's Safeguarding of Vulnerable Persons and Youth Policy. AGMARK will institute adequate mechanisms to verify age and obtain the necessary consent before processing personal data relating to a Child.

11. SENSITIVE PERSONAL DATA

AGMARK will only process Sensitive Personal Data where:

- (i) The processing is carried out in the course of AGMARK's legitimate activities, with appropriate safeguards, and relates solely to Staff or to persons who have regular contact with AGMARK, and the data is not disclosed outside AGMARK without the Consent of the Data Subject.
- (ii) The processing relates to personal data that has already been made public by the Data Subject.
- (iii) The processing is necessary for the establishment, exercise, or defence of a legal claim; for carrying out AGMARK's obligations or exercising the specific rights of AGMARK or the Data Subject; or for protecting the vital interests of the Data Subject or another person where the Data Subject is physically or legally incapable of giving Consent.

12. DATA MINIMISATION, ACCURACY AND RETENTION

AGMARK will collect and process personal data that is adequate, relevant, and limited to what is necessary for the intended purpose. Staff and Partners must not collect personal data beyond what is required for a specific programme or task, and must not access personal data which they are not authorized to access or have no reason to access.

AGMARK will take reasonable steps to ensure that the personal data it holds is accurate and, where necessary, kept up to date, and will correct or delete inaccurate or out-of-date records without undue delay.

Personal data will not be kept for longer than is necessary for the purpose for which it was collected. Staff must delete, destroy, or anonymize personal data that is no longer needed for the specific purpose for which it was collected, having regard to any retention obligations under a Donor agreement, the Data Protection Act, or other applicable law.

13. SECURITY AND SAFEGUARDING OF DATA

AGMARK will implement appropriate technical and organizational measures to protect personal data against unauthorized or unlawful processing and against accidental loss, destruction, or damage, in accordance with AGMARK's Information Security Policy and procedures. These measures include restricting access to personal data to Staff and Partners who require it for their duties, securing physical and electronic records, and ensuring that data collection devices and systems are adequately protected.

14. DATA PROTECTION IMPACT ASSESSMENTS

AGMARK will carry out a data protection impact assessment before undertaking any processing operation that is likely to result in a high risk to the rights and freedoms of a Data Subject, such as the introduction of a new programme database or a significant change in how Beneficiary data is collected or shared. The assessment will consider the nature, scope, and purpose of the processing, the risks to Data Subjects, and the safeguards needed to address those risks. It is the responsibility of the Data Protection Officer to carry out or oversee the impact assessment.

15. THE DATA PROTECTION OFFICER

AGMARK has designated a Data Protection Officer (DPO) who is responsible for:

- (i) Advising AGMARK's Staff and Partners on the requirements of this policy and applicable data protection law, including data protection impact assessments.
- (ii) Monitoring AGMARK's compliance with this policy and applicable data protection law.
- (iii) Facilitating the training and capacity building of Staff involved in data processing operations.
- (iv) Cooperating with the ODPC and other relevant regulators on matters relating to data protection.
- (v) Receiving and coordinating AGMARK's response to reports of a suspected or actual Personal Data Breach.

AGMARK's DPO is the Monitoring and Evaluation Manager, who can be contacted at info@agmark.org.

16. TRANSFERRING PERSONAL DATA ACROSS BORDERS

AGMARK operates across several African countries, and its programme data may need to be shared between its country offices, with Donors, or with Partners based in other jurisdictions. AGMARK will transfer personal data across borders only where it has:

- (i) Proof of appropriate measures for the security and protection of the personal data, including transfer to jurisdictions with commensurate data protection laws or contractual safeguards; or
- (ii) A lawful basis for the transfer, such as where it is necessary for the performance of a contract, for matters of public interest, for legal claims, to protect the vital interests of the Data Subject, or for AGMARK's legitimate interests, provided these are not outweighed by the interests, rights, and freedoms of the Data Subject.

Sensitive Personal Data will only be transferred across borders after obtaining the Consent of the Data Subject and confirming that appropriate safeguards are in place. Where personal data collected in Kenya is transferred outside Kenya, AGMARK will comply with the requirements of the Data Protection Act, 2019, including providing proof of adequate safeguards to the ODPC where required.

17. REPORTING A PERSONAL DATA BREACH

- 17.1** AGMARK places a mandatory obligation on all Staff and Partners to report any suspected or actual Personal Data Breach to the Data Protection Officer as soon as they become aware of it.
- 17.2** Where a Personal Data Breach poses a real risk of harm to a Data Subject, AGMARK will notify the ODPC without delay, and in any event within seventy-two (72) hours of becoming aware of the breach, in accordance with the Data Protection Act, 2019.
- 17.3** AGMARK will communicate the breach to the affected Data Subject(s) in writing within a reasonably practical period, unless the identity of the Data Subject cannot be established or appropriate safeguards, such as encryption, mean that no further action is required.
- 17.4** Partners and Grantees who become aware of a breach involving AGMARK's data in their custody must notify AGMARK's Data Protection Officer without delay, and in any event within forty-eight (48) hours of becoming aware of the breach.
- 17.5** AGMARK will record the facts relating to a Personal Data Breach, its effects, and the remedial action taken.

18. PARTNERS, GRANTEES AND THIRD PARTIES

AGMARK will include in its agreements with Partners a clause requiring their adherence to this policy or to a policy of an equal or higher standard. Partners and Grantees must:

- (i) Abide by this policy and institute adequate mechanisms to safeguard the privacy of individuals' personal data in their custody.
- (ii) Report any suspected or actual Personal Data Breach in accordance with Section 17 of this policy.
- (iii) Provide their employees, representatives, agents, and sub-contractors with a copy of this policy.

19. TRAINING AND AWARENESS

AGMARK will train Staff on the contents and implementation of this policy. Staff joining AGMARK will be required to familiarize themselves with this policy as part of their induction. AGMARK will develop the capacity of Staff involved in data collection and processing, particularly enumerators and data clerks, to handle personal data responsibly and in accordance with this policy.

20. ROLES AND RESPONSIBILITIES

20.1 All Staff must:

- (i) Read, understand, and comply with this policy.
- (ii) Report suspicions of a Personal Data Breach promptly to the Data Protection Officer.

20.2 All project leads and programme managers must:

- (i) Ensure that Staff and Partners they work with are aware of the contents of this policy.
- (ii) Conduct risk assessments and update controls and procedures to mitigate the risk of a Personal Data Breach.

The **Chief Executive Officer (CEO)** is responsible for ensuring that Staff, consultants, vendors, and Partner organizations are aware of this policy and are supported to implement it, and for fostering a management culture that prioritizes data protection.

AGMARK's **Board of Trustees** will ensure that adequate and effective systems and processes are in place to safeguard personal data.

21. ACCOUNTABILITY

Any Staff or Partner who processes personal data in breach of this policy will be subject to action by AGMARK as follows.

21.1 Staff

Any Staff member found to be in breach of this policy will be subject to the disciplinary process set out in AGMARK's Human Resources Policy Manual.

21.2 Partners

AGMARK may take appropriate action against a Partner found to be in breach of this policy, including termination of any contract, grant, or partnership agreement, having considered the impact of termination on programme Beneficiaries and any remedial measures undertaken by the Partner.

21.3 Donors

AGMARK will report material breaches of this policy to its Donors in accordance with Donor requirements.

22. RELATED POLICIES

This policy should be read in conjunction with:

- (i) Safeguarding of Vulnerable Persons and Youth Policy
- (ii) Ethics Policy

- (iii) Partners Code of Conduct
- (iv) Whistleblowing Policy
- (v) Human Resources Policy Manual
- (vi) Information Security Policy and procedures

23. REVIEW OF THIS POLICY

This policy will be reviewed periodically, and in any event at least every two years, to ensure it remains consistent with applicable data protection law and AGMARK's operational practices. The Data Protection Officer is responsible for ensuring that this policy is reviewed on a timely basis.

ACKNOWLEDGEMENT FORM

I confirm that I have read and understood the requirements and expectations set out under AGMARK’s Data Protection Policy (the “Data Protection Policy”).

I agree that its personnel, agents, officers, representatives, and sub-contractors shall abide by and comply with the provisions of the Data Protection Policy.

I confirm that I am duly authorized to execute this Acknowledgement Form on behalf of

Signature

Name

Capacity

Date