

REVISION 00

ISSUE 01

KENYA PLANT HEALTH INSPECTORATE SERVICE



DATA PROTECTION POLICY

JUNE 2025

VISION

Excellence in Plant Health and Quality Assurance in Agriculture

MISSION

To assure Plant Health, Quality of Agricultural inputs and produce towards a food secure nation and safe trade

CORE VALUES

Customer Focus

Professionalism

Integrity

Team Work

Innovation

TABLE OF CONTENTS

Contents

VISION.....	2
MISSION	2
CORE VALUES.....	2
ACRONYMS/ ABBREVIATIONS	5
DEFINITION OF TERMS.....	6
1.0 Part One	11
1.1 Introduction.....	11
1.2 Background.....	12
1.3 Rationale	13
1.4 Policy Objectives	13
1.5 Policy Statement	14
1.6 Scope	14
1.7 Legal And Policy Framework	14
2.0 Part Two: Policy Provisions	15
2.1 Principles Of Data Protection.....	15
2.2 Rights Of The Data Subject.....	17
2.3 Processing Of Personal Data Relating To A Minor.	22
2.4 Data Processing	22
2.5 Lawful Basis For Data Processing	23
2.6 Joint Data Controllers And Processors.....	24
2.7 Data Protection By Design And Default	24
2.8 Data Sharing And Transfer.....	24
2.9 Destruction And Retention Of Personal Data	26
2.10 Data Privacy Notice	27
2.11 Data Protection Impact Assessment (Dpia) And Reporting.	29
3.0 Part Three:	31
3.1 Policy Coordination And Implementation Framework	31
3.2 Risk Analysis	36
3.3 Monitoring And Evaluation	38

3.4 Policy Review	38
Appendix 6: Data Privacy Notice	49
A. Website Notice	49
B. Attendance Register Notice	50
Appendix 7: Monitoring And Evaluation Tool	52

ACRONYMS/ ABBREVIATIONS

DBRT	Data Breach Response Team
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EU	European Union
GDPR	General Data Protection Regulation
KEPHIS	Kenya Plant Health Inspectorate Service
M&E	Monitoring and Evaluation
ODPC	Office of Data Protection Commission
DTA	Data Transfer Agreement

DEFINITION OF TERMS

In this Policy, unless the context otherwise requires, the following words and phrases shall have the following meaning:

Anonymisation means the removal of personal identifiers from personal data so that the data subject is no longer identifiable.

Consent means any freely given, unambiguous and informed indication by a statement or by a clear positive action, signifies an agreement by the data subject to the controlling and processing of personal data.

Cross – Border Processing: means processing of data that results in data transfer beyond Kenyan jurisdiction including transfer to public clouds hosted by foreign parties.

Data means information that:

- a. Is processed by means of equipment operating automatically in response to instructions given for that purpose;
- b. Is recorded with the intention that it should be processed by means of such equipment;
- c. Is recorded as part of relevant systems;
- d. Where it does not fall under paragraphs (a), (b) or (c) forms part of an accessible record; or
- e. Is recorded and held by the Service and does not fall within any of paragraphs (a) to (d).

Data Collection means gathering of information that relates to a data subject

Data Content means any audio, video, text, images or other material a user chooses to display on the Service's platforms.

Data controller means the Kenya Plant Health Inspectorate Service.

Data Protection Officer means the person appointed under section of 24 of the Data Protection Act who is responsible for the coordination of the implementation and enforcement of data protection measures within the Service.

Data processor means any person or body processing data personal data on behalf of the Service or Service where it processes data on behalf of other controller as defined in the Data Protection Act, 2019.

Data processing means converting of data into information. This includes collecting, recording, rationalizing, storage alteration, retrieval, use, transmission, dissemination, erasure or destruction of data.

Data Protection Impact Assessment: a risk-focused assessment designed to evaluate the impact of specific data processing activities on data subjects' privacy rights and freedom, particularly in high-risk scenarios.

Data subject means a natural person whose personal data is collected, held, or processed by KEPHIS. The data subject is the individual to whom the personal data relates and who has certain rights over how their personal data is used, including the right to access, correct, or request the deletion of their data.

Data transfer means all acts that make personal data accessible to third parties outside of the Service on paper, via electronic means, on the internet through other means.

Data Transfer Agreement (DTA) means an agreement between the Service and a 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 and how the data may be used.

Employees: Shall include Service's secretariat staff employed by the KEPHIS Board.

External Stakeholder means any non – staff entity that has a contractual agreement with the Service to access information collected by Service.

Identifiable natural person means is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Identification information means details required to access the Service's website or applications including usernames, passwords or any such information.

Lawful Basis means the legitimate grounds for processing personal data, as defined by the Data Protection Act and other applicable laws.

Personal data means any information relating to an identified or identifiable natural person (data subject).

Personal data breach means 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 data means any operation or sets of operations performed on personal data whether or not by automated means, such as

- a. collection, recording, organization, rationalizing, 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.

Pseudonymisation: replacing information that identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is to be kept separately and secure.

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.

Service means Kenya Plant Health Inspectorate Service.

Third party means any natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

User means any person who accesses or uses data held by the Service.

FOREWORD

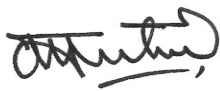
Kenya Plant Health Inspectorate Services (KEPHIS) is a regulatory body, mandated to assure plant health, quality of agricultural inputs and produce towards a food secure nation and safe trade.

In today's digital world, the protection of personal and sensitive information is not just a regulatory requirement it is a fundamental part of maintaining trust and integrity in everything we do.

This data protection policy reflects our organizations commitment to safeguarding the information entrusted to us by our employees, customers, partners and other stakeholders. We recognize the importance of complying with the Data Protection Act of 2019 and aim to uphold the high standards of privacy, transparency and accountability.

Everyone in the organization has a role to play in protecting data. This policy outlines our principles, responsibilities and procedures for handling personal information securely and lawfully.

I urge all employees, contractors and affiliates to read this policy carefully and incorporate its guidance in daily work practices. By doing so, we reinforce our culture of responsibility and ensure that, we continue to operate with trust, integrity and respect of individual rights.



Prof. Theophilus M. Mutui, PHD
MANAGING DIRECTOR

Effective Date:

1.0 PART ONE

1.1 INTRODUCTION

The Kenya Plant Health Inspectorate Service is a State Corporation established under KEPHIS Act Cap 349. The core mandate of KEPHIS is to provide plant protection, regulation of import and export of plants, plant products, and regulated articles, quality assurance of seeds and plant varieties, agricultural inputs, and produce, on behalf of the National Government, thereby promoting sustainable agricultural growth.

KEPHIS is designated as the National Plant Protection Organization (NPPO) of Kenya, with a mandate to implement international obligations and responsibilities that the State is bound to. KEPHIS enforces International Standards for Phytosanitary Measures under the International Plant Protection Convention (IPPC) to protect world's plant resources from the introduction and spread of pests that may reduce crop yield by 100%, resulting in food insecurity.

In execution of its mandate, the Service manages a huge database whose management employs a combination of both manual and technological processes. These processes entail the collection, storage, and retention of personal data for the purpose of fulfilling its mandate. As such it has digitised some of its processes to enhance efficiency and effectiveness in service delivery. KEPHIS has digitised its critical processes which may present key risks of data breaches and privacy violations. It is therefore critical to put in place robust safeguards to protect the privacy and rights of its Data Subjects.

In response to data breach and privacy violation risks, and in recognition of the right to privacy as enshrined in Article 31 of the Constitution, the Parliament of Kenya has enacted several laws to ensure the protection of personal data. The Data Protection Act is one such key statute, providing comprehensive guidelines on the handling of

personal data throughout its lifecycle.

Considering this, the Service has developed a comprehensive Data Protection Policy to serve as a key instrument in guiding its approach to data privacy, establishing accountability, and ensuring compliance with relevant laws and regulations. The policy outlines a clear framework for the collection, processing, storage, and sharing of data, while also safeguarding the rights of individuals concerning their personal information.

1.2 BACKGROUND

In today's digital and interconnected world, there is increase in reliance on digital tools, cloud services, and data-driven decision-making by organizations. This has subsequently raised concerns over the security of personal data stored by institutions. In an effort to address these concerns, governments have enacted data protection regulations. For instance, in 2018, the European Union (EU) implemented the General Data Protection Regulation (GDPR), setting rules on how companies must manage personal data. Following suit, Kenya introduced its own Data Protection Act in 2019. These regulations aim to safeguard individuals' privacy by enforcing responsible data processing practices such as upholding principles of lawful processing, minimizing data collection, ensuring data accuracy, and implementing security measures to protect personal data.

The Service recognizes that the protection of individuals through lawful, legitimate and responsible processing and use of personal data is a fundamental human right. To this end, while the Service manages a huge set of personal data and has digitized some of its processes, it continuously adopts best practices to ensure that the data it collects is processed in a manner that promotes the principles of data protection and the rights of the data subjects.

The adoption and implementation of the Policy shall not only ensure compliance with

legal obligations but also build trust with employees and stakeholders, reinforcing the Service's commitment to maintaining the highest standards of data security and privacy.

1.3 RATIONALE

Cognizant of the right to privacy and the right to access to information under Article 31 and 35 of the Constitution respectively, the Service has a responsibility to ensure that the personal data it collects is processed within these rights and the provisions of the relevant legislations.

It is on this basis that the Service as a Data Controller and Data Processor has identified a need for a comprehensive data protection policy to serve as an instrument to guide its approach to data protection. This policy will provide a framework to ensure that data collection, processing, retention, sharing, erasure and deletion aligns to the principles of data protection.

1.4 POLICY OBJECTIVES

1.4.1 General objective

The general objective of the policy is to establish a framework for the collection, processing, retention, sharing, erasure and deletion of personal and sensitive data while ensuring compliance with the legal and regulatory requirements.

1.4.2 Specific objectives

The specific objectives of this policy are to: -

- (a) Provide clear guidelines on how personal data is collected, processed, retained and shared;
- (b) Identify, assess and mitigate data security risks;
- (c) Provide guidelines on how to adhere to the principles of data protection; and
- (d) Define roles and responsibilities on data protection in the Service.

1.5 POLICY STATEMENT

The Service is committed to implementing appropriate measures to ensure that personal data is collected, processed, retained, and shared responsibly and securely. To this end, the Service will maintain the highest standards of data protection by adhering to the principles of data protection and implementation of the provisions in this policy. Further, it is committed to protecting personal data of its subjects from unauthorized access and use.

1.6 SCOPE

This policy shall apply to data subjects, employees, and third parties involved in handling personal data collected and processed by the Service. It covers instances where the Service acts as a data controller or data processor ensuring compliance with applicable data protection laws, contractual obligations, and the rights of data subjects in all such roles.

1.7 LEGAL AND POLICY FRAMEWORK

The Policy is anchored in the following laws and regulations:

- (a) The Constitution of Kenya 2010;

- (b) Kenya Plant Health Inspectorate Service Act, Cap 349;
- (c) The Data Protection Act, Cap 411C;
- (d) Access to Information Act, Cap 7M;
- (e) Kenya Information and Communications Act, Cap 411A;
- (f) Computer Misuse and Cybercrimes Act, Cap 79C;
- (g) Public Archives and Documentations Services Act, Cap 19S;
- (h) Records Disposal Act Cap 14; and
- (i) All other prevailing provisions of law.

2.0 PART TWO: POLICY PROVISIONS

2.1 Principles of Data Protection

The following key principles shall be adhered to in implementing this Policy.

KEPHIS will ensure: -

- a) **Data accuracy:** Suitable steps must be taken to ensure that personal data is accurate and complete.
- b) **Data confidentiality and security:** Personal data shall be treated with utmost confidentiality. Data shall be secured with suitable organizational and technical measures to prevent unauthorized access, illegal processing, distribution, loss, modification or destruction.
- c) **Data minimization and minimalism:** The Service shall determine whether and to what extent the processing of personal data is necessary in order to achieve the purpose for collection. The Service shall limit the collection of personal data to what is relevant and necessary for the purpose of collection. Personal data provided by individuals that is no longer needed after the expiration of legal or business process- related periods may be disposed or destructed unless there is justification for continued retention.
- d) **Fairness and lawfulness:** When processing personal data, individual rights of the data subjects shall be recognized and protected. Personal data shall be collected and processed in a legal and fair manner.
- e) **Restriction to a specific purpose:** Personal data shall be processed only for the purpose that is set out in the applicable laws before the data is collected. Subsequent changes to the purpose shall only be allowed to a limited extent and shall require written substantiation to the data subject by the data processor.

- f) **Transparency:** Personal data may be collected directly or indirectly. Where the data is collected directly, the data subject shall be informed of the purpose for which the data is collected and the third parties or categories of third parties to whom the data might be transmitted, if any.
- g) **Cross- border transfer:** Adequate safeguards and consent from the data subject shall be obtained before transfer of data outside Kenya to ensure data protection.

2.2 RIGHTS OF THE DATA SUBJECT

Subject to legal and contractual expectations, a data subject has rights under Data Protection Act, 2019 in relation to personal data. These include the right to: -

2.2.1 *Right to be informed*

Data subjects shall have the right to be informed of the collection, processing, and intended use of their personal data. The Service shall through the Privacy Notice provide clear, concise, and accessible information on: -

1. The purposes for which the data is being collected and processed;
2. The legal basis for processing the data;
3. Any third parties with whom the data may be shared; and
4. The rights available to the data subject.

2.2.2 *Right to access*

2.1.1.1 A data subject shall have the right to request and obtain confirmation from the Service on how their personal data is being processed. The data subject may request access to: -

- i. The personal data being processed;
- ii. The purpose of processing;
- iii. The recipients or categories of recipients to whom the data has been disclosed; and
- iv. The period for which the data will be stored.

2.1.1.2 A request to access personal data shall be in **Appendix 1** under the first schedule.

2.1.1.3 The Service shall respond to such a request for access to data within a period of 7 days.

2.2.3 *Right to object to processing*

1. The data subject shall have the right to object to processing of all or part of their personal data, for a specified purpose or in a specified manner. The data subject may object to the processing of their personal data in the following circumstances: -

- (a) When processing is based on legitimate interests or public interest of the Service as opposed to the data subject;
- (b) If personal data is processed for direct marketing purposes; and
- (c) When data processing involves automated decision-making, including profiling.

2. A request to object to processing shall be done in **Appendix 2**.

3. The Service may comply with the request to object to processing of personal data within 14 days upon receipt of the request form, filled in the prescribed manner.
4. Notwithstanding the provisions of clause 2.2.3.3 above, a request to exercise the right to object where processing is for direct marketing purposes shall be absolute.

2.2.4 *Right to Restriction of Processing*

1. A data subject may request the restriction of processing of personal data under the following circumstances:
 - (a) If they contest the accuracy of the personal data.
 - (b) If the Service no longer needs the data for processing, but the data subject requires it for legal claims.
2. A request to restrict processing shall be done in **Appendix 2** under the first schedule.

2.2.5 *Right to correction of false or misleading data*

1. A data subject shall have the right to request for correction of inaccurate, incomplete, outdated, untrue or misleading personal data held by the Service.
2. A request to correction of false or misleading data shall be done in **Appendix 3** under the first schedule.
3. The Service will endeavor to rectify the sought correction within a period of 14 days.
4. Where the Service is of the opinion that the request for correction is unjustified, the Service shall give reasons in writing, to the data subject for such refusal within 14 days.

2.2.6 *Right to deletion of personal data*

1. A data subject shall have the right to request for the deletion of their personal data in the event that: -
 - i. The data is no longer necessary for the purpose it was collected;
 - ii. The data subject withdraws consent, and there is no other legal basis for processing;
 - iii. The data has been unlawfully processed; and
 - iv. The data must be erased to comply with legal obligations.
2. A request for deletion of personal data shall be done in **Appendix 4**.
3. Where personal data is required for the purposes of evidence, the Service shall, instead of deleting/erasing/rectifying such data, restrict its processing and inform the data subject within 14 days.

2.2.7 *Right to be forgotten*

1. Data subject may request to have their data erased or destroyed and that they be completely forgotten in the following instances: -
 - (a) Where the data subject objects to the processing of their data and there is no overriding legitimate interest;
 - (b) Where the data is no longer necessary for the purpose which it was collected;
 - (c) When consent is withdrawn where it was the lawful basis; or
 - (d) The erasure is necessary to comply with a legal obligation.
2. A request to be forgotten shall be done in **Appendix 4**.

3. The Service will endeavor to comply with the request to be forgotten within a period of 14 days, and in any event as soon as practically possible.
4. Where personal data is required for the purposes of evidence, the Service shall, instead of deleting/erasing such data or forgetting such data subject, restrict its processing and inform the data subject within a reasonable time.

2.2.8 *Right to data portability*

1. A data subject shall have the right to receive personal data concerning them in a structured, commonly used and machine-readable format.
2. Where technically feasible, the data subject shall have the right to have this data transmitted to another controller without hindrance.
3. A request for data portability shall be done in **Appendix 5**. The Service shall upon processing the request, have the data ported within 30 days from the request.
4. Where a request for portability is declined, the Service shall inform the data subject of the reasons thereof in writing within 14 days.

2.2.9 *Right Not to Be Subject to Automated Decision-Making*

1. Data subjects shall have the right not to be subjected to a decision based solely on automated processing, including profiling, if such decisions significantly affect them.
2. The Service shall however reserve the right to undertake processing of data through an automated process if: -
 - (a) The processing is necessary for entering into or performing a contract.
 - (b) The data subject has given explicit consent; and

(c) There is a legal requirement for automated decision-making.

2.3 Processing of personal data relating to a minor.

The Service shall process personal data relating to minors in a manner that protects and advances the rights and best interest of the minor.

2.4 DATA PROCESSING

2.4.1 Data Collection

1. The Service shall: -

(a) In collection of personal data adhere to the principles of data protection.

(b) Collect personal data directly from data subject

2.4.2 Notwithstanding the clause above, the Service upon informing the data subject within 14 days may collect personal data indirectly where: -

(a) Data is contained in a public record;

(b) The data subject has deliberately made the data public;

(c) The data subject has consented to the collection from another source;

(d) The data subject has an incapacity and the guardian appointed has consented to the collection from another source;

(e) The collection from another source would not prejudice the interests of the data subject; and

(f) The collection of personal data from another source is necessary for:

-

i. The prevention, detection, investigation, prosecution and punishment of crime;

ii. The enforcement of a law which imposes a pecuniary penalty; or

iii. The protection of the interests of the data subject or another person.

2.5 Lawful Basis for Data Processing

The Service shall process personal data to: -

(a) Perform contractual obligation where the data subject is a party to the contract;

(b) Comply with any legal obligation to which the Service is subject;

(c) Protect the vital interests of the data subject or another natural person;

(d) Perform a task carried out in the public interest or in the exercise of official authority vested in the Service;

(e) Fulfil its legitimate interests within the tenets of Data Protection principles;

(f) Where the data subject has consented to the processing of personal data by the Service, s/he may withdraw such consent at any time. The withdrawal of the

consent to process data shall not affect the lawfulness of data processing conducted before the withdrawal; and

(g) Carry out historical, statistical, journalistic and scientific research.

2.6 Joint Data Controllers and Processors

Instances where the Service engages another data controller or processors both parties shall: -

- (a) Determine the purpose(s) of processing personal data.
- (b) Determine the respective responsibilities for compliance and exercise the rights of the data subject in a transparent manner.

2.7 Data protection by design and default

The Service shall implement privacy by design and default in all its data management systems and processes. In doing this, the Service shall among others:-

- (a) Conduct privacy and information audit and risk assessment at each stage of every project or initiative involving processing of personal data.
- (b) Apply appropriate Personal Data security controls such as encryption, anonymization and Pseudonymisation of Personal Data.

2.8 Data Sharing and Transfer

- 2.8.1 The Service may share or exchange personal data collected, upon request in writing by another Data Controller, Data Processor or third party and upon

consideration of the advisory of the Data Protection Officer and approval of the Commissioner. Data sharing may include: -

- (a) Providing personal data to a third party;
- (b) Receiving personal data from a Data Controller or Data Processor pursuant to a Data Sharing Agreement;
- (c) Separate or joint initiatives by the Service and a Data Controller or Data Processor to pool Personal Data making the data available to each other or a third-party subject to a Data Sharing Agreement; and
- (d) Routine data sharing between the Service and Data Controller on a regular or pre-planned basis.

2.8.2 The Service shall not transfer Personal Data in a manner that is incompatible with the principles of data protection.

2.8.3 The Data Transfer Agreements shall among others: -

- (a) Highlight the purpose(s) of the Personal Data transfer;
- (b) Provide the legal basis or authority that allows collection of Personal Data;
- (c) List the specific Personal Data elements that shall be shared;
- (d) Indicate how the data shared shall be used by the other party;
- (e) Require the other party to have security measures in place to negate data breach;

(f) Indicate the period for data retention and the mode of destruction of the data; and

(g) Indicate the reporting procedure in the event of a data breach.

2.8.4 The Service may transfer Personal Data outside Kenya only when: -

(a) There is proof of appropriate measures for security and protection of Personal Data, in the receiving country in line with Data Protection (General) Regulations; or

(b) The Data Protection Commissioner has approved the request for transfer of the Personal Data outside Kenya; or

(c) The Service has received consent from the Data Subject to transfer the Data outside Kenya; or

(d) The transfer outside Kenya is necessary based on a legitimate reason.

2.9 Destruction and Retention of Personal Data

The Service shall: -

(a) Retain personal data for as long as reasonably necessary for the purpose for which data is processed;

(b) Maintain a Retention Schedule of personal data to be reviewed once two years with a view to identifying personal data that is no longer required to be retained; and

(c) Dispose off Personal Data in a way that protects the rights and privacy of Data Subjects.

2.10 Data Privacy Notice

Every data subject providing information to the Service or whose data is collected as a result of seeking services from the Service consents and agrees with the terms of the Data Privacy Notice contained in **APPENDIX 6**.

2.10.1 Data Breach

- a. In line with regulatory requirements, the Service shall report to the Data Protection Commission any data breach within 72 hours of being aware.
- b. The Service shall communicate any data breach to the data subject within 14 days unless the identity of the data subject cannot be established.

2.10.2 Internal Reporting

All staff shall immediately report confirmed data breaches to the data protection officer through Email: dataprotectionofficer@kephis.org.

Reports must include: -

- (a) Exact date and time of detection;
- (b) Specific systems/data affected;
- (c) Estimated number of impacted data subjects; and
- (d) Initial containment measures taken.

2.10.3 Reporting of Data Breach to the ODPC

The Service shall within seventy-two (72) hours notify the Data Protection Commissioner of a data breach. Where the notification is not done within seventy-two (72) hours, the Service shall provide reasons for the delay.

2.10.4 Notification to the data subject

The Service shall inform the data subject of the data breach in writing within reasonable time, unless the identity of the data subject cannot be verified or prior to the breach the Service had put in place appropriate security safeguards either by design or default.

2.10.5 Response to data breach

2.10.5.1 The Service shall establish a Data Breach Response Team (DBRT), comprising of the following: -

- (a) DPO
- (b) Representative from ICT Department
- (c) Representative from Legal Department
- (d) Representative from the affected Directorate/ Department
- (e) Data protection Champion from relevant directorate/ department

2.10.5.2 The DBRT shall: -

- (a) Convene immediately following a reported breach incidence;
- (b) Undertake a root cause analysis and assess the extent of the breach;
- (c) Isolate, restore and recover the compromised systems as stipulated in the Service's Disaster Recovery Plan; and

- (d) Develop a corrective action plan.
- (e) Prepare and submit a breach assessment report to the Managing Director within 24 hours.
- (f) Carry out a post-incident reviews after 14 days of the incident.

2.11 Data Protection Impact Assessment (DPIA) and Reporting.

2.11.1 The Service shall conduct DPIA to ensure that its processing activities align to the principles of data protection and rights of data subjects.

2.11.2 The Service shall within sixty days, prior to, processing, submit DPIA to the Office of the Data Protection Commissioner (ODPC) where: -

- (a) Sensitive and personal data is processed at a large scale;
- (b) Automated decision-making with legal effects is being employed such as employee profiling;
- (c) Systematic monitoring is being employed in the Service;
- (d) Innovations or new technologies are being introduced or major changes to existing processes;
- (e) Matching or combining datasets, where personal data originating from two or more data processing

operations for purposes and/or by different data controllers; and

- (f) When the processing in itself prevents data subjects from exercising a right.

2.11.3 DPIA shall be conducted annually as per the template outlined in the second **Appendix 7**

3.0 PART THREE:

3.1 POLICY COORDINATION AND IMPLEMENTATION FRAMEWORK

3.1.1 *The Service*

- a. The Service is responsible for establishing policies and procedures in order to comply with the relevant and applicable data protection in law (s).
- b. The Service through the Legal Service Directorate shall be responsible for ensuring that all staff within their area of responsibility comply with this policy and implement appropriate practices, processes, controls and trainings to ensure compliance.
- c. The Service shall appoint a Data Protection Officer who will responsible for: -
 - i. Advise the Service 's staff on requirements for data protection, including data protection impact assessments;
 - ii. Monitoring that the Service is compliant with the legal requirements on data protection;
 - iii. Facilitate capacity building of staff involved in data processing operations;
 - iv. Cooperate with external regulators on matters relating to data protection. KEPHIS's DPO can be contacted via the email; director@kephis.org
 - v. Notifying the Data Protection Commission of any data breach; and
 - vi. Resolving personal data complaints in accordance with the data protection (complaints handling and enforcement procedures) Regulations 2021.

- d. The Service shall not sell, trade, rent or otherwise share a data subject's personal data without consent, except as otherwise stated in this policy, bilateral agreements or statutory obligations.
- e. The Service will conduct regular audits and monitoring of its data protection and security measures to ensure compliance with this policy and applicable laws.

3.1.2 *The Board*

The Board shall: -

- (a) Provide oversight on implementation of this policy
- (b) Review the policy

3.1.3 *Managing Director*

The Managing Director shall: -

- (a) Establish the office of the DPO;
- (b) Appoint DPO and the DBRT;
- (c) Coordinate the implementation of this policy;
- (d) Provide resources for the implementation of the policy;
- (e) Appoint the data protection champions from every Directorate/ department;
and
- (f) Communicate the policy to the employees.

3.1.4 *Management*

The Management shall ensure: -

- (a) Implementation of this policy in their respective Directorate/ departments;
- (b) Awareness creation of the provisions of this policy for staff, consultants, and third parties operating under them;
- (c) Data under their jurisdiction are promptly updated and well maintained to ensure data accuracy;

- (d) Minimization of data by collecting relevant data limited to what is necessary in relation to the purposes for which it is required;
- (e) Processes to improve the quality and security of data in the service areas are in place; and
- (f) Maintenance of data breach registers for their Directorates/ departments.

3.1.5 DPO

The Data Protection Officer shall: -

- (a) Advise the Service on the data processing requirements under the Kenya Data Protection Act, 2019 or any other written law;
- (b) Serve as the point of contact and liaison within the Service for members of staff, Office of the Data Commission and any other relevant public entities on issues related to data protection;
- (c) Monitor the Service's performance and compliance with the Data Protection Act and related policies;
- (d) Lead Officer in the implementation of the Data Protection Policy;
- (e) Facilitate the provisions of reports and or information to the Office of the Data Commission as and when required;
- (f) Respond to data subject access requests and manage data subject rights;
- (g) Create and maintain a register of data processing operations/activities in the Service;
- (h) Advise and coordinate Data Protection Impact Assessment;

- (i) Update and advise the Service on its compliance status with statutory and regulatory requirements on Data Protection;
- (j) Conduct and coordinate training and raising awareness about data protection among employees; and
- (k) Keep abreast of any changes to relevant laws and regulations on data protection and advise the Service accordingly.

3.1.6 *Data Protection Champions*

The Data Protection Champion shall: -

- (a) Serve as the point of contact between the Directorate/ Department and Data Protection Officer;
- (b) Monitor the level of compliance of the Directorate/ Department processes to data protection requirements;
- (c) Develop and maintain a register of data processing operations/activities in the Directorate;
- (d) Conduct and coordinate training and raising awareness about data protection among employees in the Directorate/ Department;
- (e) Identify data protection training needs at the Directorate/ Department; and
- (f) Monitor and advise the DPO on the need for DPIA on Directorate/ Department projects and processes.

3.1.7 Employees

The Employees shall: -

- (a) Familiarize and adhere to the provisions of the policy;
- (b) Provide accurate personal data;
- (c) Process personal data in accordance with the provisions of the policy;
- (d) Report data breach to the DPO immediately;
- (e) Personal data is not disclosed either verbally or in writing, accidentally or otherwise, to any authorized person;
- (f) Personal data is kept in accordance with the Service's records management policy and the retention schedule **APPENDIX 8**;
- (g) Any queries or data breach regarding personal data are directed to the Data Protection Officer; and
- (h) External consultants involved in processing of personal data comply with this policy.

3.1.8 External Stakeholders

The External Stakeholders shall: -

- (a) Any personal data collected or processed in the course of work undertaken for the Service is kept securely and confidentially;
- (b) All personal data is returned to the Service upon completion of the work, including copies that may have been made. Alternatively, the data should be securely destroyed and the Service receives written notification in this regard from the contractor or external stakeholders;
- (c) Seek written consent from the Service prior to any disclosure of personal data to any other organization or any person who is not a direct employee of the contractor; and

- (d) Any personal data made available by the Service, or collected in the course of the work, should neither be stored nor processed outside the Service unless authorized.

3.1.9 Consequences of Non-Compliance:

- a. Failure to comply with this Policy by the Service staff may constitute grounds for disciplinary action in accordance with the KEPHIS Code of Conduct and may include termination of employment
- b. Failure to comply with this Policy by external stakeholders, may constitute grounds for termination of contract or affiliation.
- c. The Service may institute legal action against any party in breach of its policy.

3.2 Risk analysis

The impact of this policy will significantly depend on how the Service effectively mitigates the risks in its implementation. This section presents a brief analysis of the risks and mitigations in the implementation of this policy.

Table 1: Risk Matrix

No.	Risk identity and description	Consequences	Mitigation Measures
1.	Non-Compliance: Failure to meet regulatory requirements	Fines and legal actions against the Service	i. Periodic monitoring of implementation of the policy through scheduled compliance audits. ii. Strong encryption and multi-factor authentication .
2.	Resistance to change: Employees and stakeholders may resist new protocols	Non-adherence to the provisions of the policy and by extension the	i. Review the existing operating procedures to mainstream them with

No.	Risk identity and description	Consequences	Mitigation Measures
		DPA, Unauthorized access	the data protection requirements ii. Continuously sensitize staff and stakeholders on the provisions of this policy. iii. Vetting third parties for regulatory compliance
3.	Cyber security risks: Potential threats and vulnerabilities against data management systems	Unauthorized access, data breaches, financial loss, or disruption of Services digital systems, unauthorized cross border transfer	i. Implement multi-factor authentication for data handlers ii. Regularly updating of fire walls and data protection software iii. Train employees on cybersecurity best practices iv. Use firewalls, intrusion detection systems, and endpoint protection v. Conduct regular security audits and penetration testing vi. Encrypt sensitive data and use strong password policies vii. Data masking
4.	Data Breaches	Unauthorized access, Financial loss, Sanctions, Legal charges, Reputational damage,	i. Use of access controls ii. Physical restrictions iii. Implementation of the DP policy

No.	Risk identity and description	Consequences	Mitigation Measures
			iv. Regular access control reviews

3.3 Monitoring and Evaluation

The Service will monitor the implementation of this policy by conducting regular reviews, at least once a year or when significant changes happens, such as new regulations or technological updates. The Data Protection Officer (DPO) will oversee this process, ensuring that the policy aligns with the legal requirements and policy provisions. Monitoring and Evaluation shall be conducted using the tool in **Appendix 7**.

3.4 Policy review

This policy framework will be reviewed after every three (3) years or as and when need arises.

Appendix 1: Request for access to Personal Data Form

KEPHIS/Dept/Form/DP/01



REQUEST FOR ACCESS TO PERSONAL DATA FORM

1. Applicant Details

Full Name: _____

National ID/Passport No.: _____

PF Number (if applicable): _____

Postal Address: _____

Email Address: _____

Phone Number: _____

2. Details of the Data Requested

(Please specify the personal data you are requesting access to.)

.....

.....

3. Purpose of the Request

(Please indicate the reason for requesting access to the data.)

☐ Verification of personal information

☐ Correction of inaccurate data

☐ Exercising rights under the Data Protection Act

☐ Other (please specify): _____

4. Preferred Mode of Access

(Please select how you would like to receive the data.)

☐ Email

☐ Hard Copy Collection

☐ Other (please specify): _____

5. Declaration

I _____ confirm that the information provided in this request is accurate and that I am the data subject or a legally authorized representative. I understand that KEPHIS may require proof of identity before processing this request.

Signature: _____

Date: _____

6. For Official Use Only

Received By: _____

Designation: _____ **Date Received:**

Action Taken:

☐ Request Approved

☐ Request Denied (Reason: _____)

Notes:

1. KEPHIS may request additional documentation to verify identity.
2. Any fees applicable for processing the request will be communicated in advance.

Appendix 2: Request to Object or Restrict Processing
KEPHIS/Dept/Form/DP/02



REQUEST TO OBJECT OR RESTRICT PROCESSING

1. Applicant Details

Full Name: _____

National ID/Passport No.: _____

PF Number (if applicable): _____

Postal Address: _____

Email Address: _____

Phone Number: _____

2. Nature of request

(select the specific right)

☐ Restriction

☐ Objection

State the justification and provide supporting documentation

3. Declaration:

I confirm that the information provided in this request is accurate and true to the best of my knowledge.

Full Name: _____

Your Signature: _____

4. For Official Use Only

Received By: _____

Designation: _____ **Date Received:**

Action Taken:

☐ Request Approved

☐ Request Denied (Reason: _____)

Notes:

1. KEPHIS may request additional documentation to verify identity.
2. Any fees applicable for processing the request will be communicated in advance. request will be communicated in advance.

Appendix 3: Request for Correction of Personal Data

KEPHIS/Dept/Form/DP/03



REQUEST FOR CORRECTION OF PERSONAL DATA

1. Applicant Details

Full Name: _____

National ID/Passport No.: _____

PF Number (if applicable): _____

Postal Address: _____

Email Address: _____

Phone Number: _____

I request the correction of my personal data below:

No.	Personal data to be corrected	Proposed change	Reasons for the proposed change and supporting documents
1.			
2.			

NB: *Any attempt to rectify personal data through misrepresentation may result in prosecution*

2. Declaration:

I confirm that the information provided in this request is accurate and true to the best of my knowledge.

Full Name: _____

Your Signature: _____

3. For Official Use Only

Received By: _____

Designation: _____ **Date Received:**

Action Taken:

☐ Request Approved

☐ Request Denied (Reason: _____)

Notes:

1. KEPHIS may request additional documentation to verify identity.
2. Any fees applicable for processing the request will be communicated in advance.

Appendix 4: Request for Deletion of Personal Data or to be Forgotten
KEPHIS/Dept/Form/DP/04



REQUEST FOR DELETION OF PERSONAL DATA OR TO BE FORGOTTEN

1. Applicant Details

Full Name: _____

National ID/Passport No.: _____

PF Number (if applicable): _____

Postal Address: _____

Email Address: _____

Phone Number: _____

2. Request for Deletion of Personal Data or to be forgotten

I request (*Tick where appropriate*)

- ☐ Deletion of my personal data (*Provide the specific personal data*)
- ☐ To be forgotten

3. Reason for Request

(*Select the applicable reason*)

- ☐ The data is no longer necessary for the purposes for which it was collected.
- ☐ I withdraw my consent, and there is no other legal ground for processing.
- ☐ The data was collected unlawfully.
- ☐ The data is inaccurate and I request its removal.
- ☐ Other (please specify): _____

NB: *Any attempt to delete personal data through misrepresentation may result in prosecution*

4. Declaration:

I confirm that the information provided in this request is accurate and true to the best of my knowledge.

Full Name: _____

Your Signature: _____

5. For Official Use Only

Received By: _____

Designation: _____ **Date Received:**

Action Taken:

☐ Request Approved

☐ Request Denied (Reason: _____)

Notes:

1. KEPHIS may request additional documentation to verify identity.
2. Any fees applicable for processing the request will be communicated in advance.

Appendix 5: Request for Data Portability

KEPHIS/Dept/Form/DP/05



REQUEST FOR DATA PORTABILITY

1. Applicant Details

Full Name: _____

National ID/Passport No.: _____

PF Number (if applicable): _____

Postal Address: _____

Email Address: _____

Phone Number: _____

2. Nature of Data Requested for Portability (Tick as applicable):

- ☐ Employment Records
- ☐ Payroll Information
- ☐ Pension and Benefits Data
- ☐ Disciplinary Records
- ☐ Training & Professional Development Records
- ☐ Other (Specify): _____

3. Preferred Format for Data Transfer (if applicable):

- ☐ Hard Copy
- ☐ Soft Copy
- ☐ Other (Specify): _____

4. Recipient of the Data:

- ☐ Name of Organization/Institution/Individual: _____
- ☐ Contact Details: _____
- ☐ Email: _____

5. Declaration:

I confirm that the information provided in this request is accurate and true to the best of my knowledge.

Full Name: _____

Your Signature: _____

6. For Official Use Only

Received By: _____

Designation: _____ **Date Received:**

Action Taken:

- ☐ Request Approved
- ☐ Request Denied (Reason: _____)

Notes:

1. KEPHIS may request additional documentation to verify identity.
2. Any fees applicable for processing the request will be communicated in advance.

APPENDIX 6: DATA PRIVACY NOTICE

A. WEBSITE NOTICE

"By using the Service's Systems, website and accessing the Services through the systems and websites, I acknowledge that I have read and understood and agree to the contents of this privacy notice.

By submitting data or information to Kenya Plant Health Inspectorate Service (KEPHIS), Center of Phytosanitary Excellence (COPE) or any of KEPHIS's website/ systems, I give consent that all personal data that I submit or that is collected by the Service shall be processed by the Service for the purposes described in statutory provisions or laws enacted by the Parliament of Kenya or in fulfilment of Kenya's obligations under international conventions on exchange of information.

In the event that the Service undergoes a business transformation, I acknowledge and consent that my personal data may be among the assets to be transferred to new platforms or entities.

I hereby consent to the collection, use and processing of my personal data by the Service in carrying out its mandate under the Laws of Kenya."

C. KENYA PLANT HEALTH INSPECTORATE SERVICE (KEPHIS)

[illegible]

KEPHIS SIGN- OFF FORM FOR THE DATA PROTECTION AND PRIVACY POLICY

I.....of P/NO.....
acknowledge that I have read, understood and agree to comply with this Policy.

Staff's signature.....

Date.....

APPENDIX 7: MONITORING AND EVALUATION TOOL

M & E TOOL

Activity	KPI	Target	Achievement	Variance	Causes	Corrective actions	Outcome	Impact

APPENDIX 8: KEPHIS DATA RETENTION SCHEDULE

S/No.	Stakeholders	Personal Data Collected	Purpose Of Retention	Retention Period	Audit	Action After Audit
1.	COPE		Administration, Information Education and Communication	Permanent	Annual	Update and Archive after seven (7) years
2.	Institutional Clients		Administration, Marketing	Permanent	Annual	Update and Archive after seven (7) years
3.	Individual Clients		Administration	Permanent	Annual	Update and Archive after seven (7) years
4.	Suppliers, Professional Bodies		Administration	Permanent	Annual	Update and Archive after seven (7) years
5.	Development Partners		Information Education and Communication, Administration	Permanent	Annual	Update and Archive after seven (7) years
6.	Media and Content Creators		Information Education and Communication	Permanent	Annual	Update and Archive after seven (7) years upon exit from the Service
7.	General Public		Administration	Permanent	Annual	Update and Archive after seven (7) years upon exit from the Service
8.	KEPHIS Board, Staff		Management of Employment	Permanent	Annual	Update and Archive after

S/No.	Stakeholders	Personal Data Collected	Purpose Of Retention	Retention Period	Audit	Action After Audit
			relationship and Employee Benefit processing			seven (7) years upon exit from the Service