1. TITLE: NSPRI'S DATA PRIVACY AND PROTECTION POLICY-DRAFT

2. Introduction

As domiciled in the Federal Ministry of Agriculture and Food Security (FMAFS), one of the mandates of the Nigerian Stored Products Research Institute (NSPRI) is to "create a database for published research findings and human resources directory in postharvest science". Further, it could be inferred that in fulfilling its other specific mandates and core functions related to research, extension and training, the Institute invariably must gather, evaluate, and improve access to data and information, in areas related to the provision of agricultural postharvest solutions in Nigeria.

Ergo, data is a strategic tool for achieving the overall mandate of NSPRI. A data protection policy is indispensable to ensure the protection of data processed by NSPRI and guarantee its value, use without undermining or putting it at risk. Any data collected, processed, and used by NSPRI, or transferred to a third party by NSPRI, must be managed correctly and consistently during the data lifecycle, that is from initial collection, storage to deletion. Unauthorized disclosures, misuse, and improper processing of data, as well as the processing of poor-quality data, exposes the NSPRI to legal, operational, and reputational risks. A properly implemented data protection policy contributes to enhancing trust in the Institute. It is imperative that any data held by NSPRI, or entrusted by NSPRI to a third party, is appropriately protected.

3. Statement

With the purpose of mitigating risks and enhancing protection, this present policy delineates NSPRI's Data protection First Principle. These all-embracing principles are in sync with those of Agricultural Research Council of Nigeria (ARCN), the supervising agency and other regional, national, and international data protection standards and are applicable to the whole lifecycle of data processing, that is, collection, use, storage, and deletion.

Data protection FIRST principles are:-

- Fairness
- Integrity
- Responsibility
- Security
- Transparency

The Data protection FIRST Principles allow for flexibility in application, and together with responsibilities arising from them, are neutral with respect to technology. Personnel should interpret the principles into measures and tools appropriate to their needs while, simultaneously, ensuring a proportionate level of protection of the data that they process. Other operational guidelines addressing specific categories of activities necessitating data processing are included in this policy.

Principles of data protection

The data privacy and protection in NSPRI is centred on Fairness, Integrity, Responsibility, Security, and Transparency outlined as follows;

Fairness

Fairness means NSPRI will collect and process data in a way that is perceived to be reasonable to data provider(s). Legitimate basis for collection and processing of data as well as specific purposes will be established in all circumstances. Only minimum data element necessary for the specified purpose will be collected**.** All data collected shall not be retained after its purpose has been fulfilled**.**

NSPRI staff will only collect and process data as part of NSPRI activities within the context of her mandate in line with ARCN's guidelines. In relation to data collection and processing, legitimate basis include

securing informed consent, oral or written, of data provider prior to collection and processing; protecting interests of data provider if informed consent is unobtainable; and implementing agreements reached prior to collection and processing of data.

- The specific purpose for collection and processing of data should be distinctly defined. Only data amount required to accomplish a specific objective should be collected and processed. Any data that is adjudged nonessential, immaterial or excessive in relation to its particular purpose should not be collected or processed.
- Data will only be retained for a specified duration to achieve the purpose for which the data was collected. All data deemed to have achieved it purpose will be deleted from all databases associated with NSPRI or anonymised within a reasonable period except when being used for statistical research or archive purposes.
- Appropriate standards, processes and tools must be implemented by NSPRI personnel for retention and deletion of data collected and or processed.
- Any third-party receiving data from NSPRI must agree to use the data collected or process for the specified purpose and return or delete the received data from their database once the purpose of the data has been achieved or upon the expiration or termination of their contractual agreement with NSPRI. However, the third party can continue to use such data with the explicit consent of the data provider.

Integrity

Integrity connotes employing practices intended to safeguard the overall accuracy of the data in order to enhance effective analysis and use. All members of staff should implement measures that guarantee accuracy and reliability pre, during, and post data collection. All reasonable steps must be taken to make certain the accuracy of the data. Any data determined to be imprecise or false would be subjected to a review process that rectifies or removes it

- Concerned members of staff are exclusively responsible and liable for the accuracy of the data they process.
- All reasonable steps must be taken to obtain and submit only accurate data, and promptly remove or remedy any inaccurate data.
- Institute periodical appraisal procedures to enhance accuracy of data by preventing or reducing errors or irregularities.

Responsibility

All members of staff must comply with the Nigerian Stored Products Research Institute Data Protection policy and must be able to make compliance to the Policy evident, as well as to related guidelines and procedures defined by NSPRI.

Satisfactory and balanced measures, regularly revised, and updated as necessary, must be put in place to demonstrate that the processing of data is executed in line with this Policy. In advance of data processing, the operation must be designed to preclude or lessen risks to data providers and to the Institute. Only data required to accomplish the specific aim should be collected. While specific data processing activities determine what constitutes proof, actions that may serve as proof of compliance include but not limited to the following:

- Preservation of up-to-date records of processing activities which comprises, at the barest minimum, information on the reason for processing, the data processed, the confidentiality level, and recipients of the data (both internal and external), agreed retention periods and the security measures adopted. Before processing data, a data protection impact assessment which identifies,

addresses, and lessens risks for the data provider, or the Institute must be carried out. Likelihood and severity of any possible harm must be determined by concerned members of staff and high-risk processing operations must be reported for advice and guidance on possible mitigation procedures and implementation.

- Data processing must be designed so as to forestall, eliminate, or lessen identified risks.
- Implement processes and procedures for handling and responding to requests from data providers. Processes and procedures for handling and responding to requests from data providers must be implemented.
- Processes, methods and techniques that safeguard a level of security equivalent to the confidentiality level required must be implemented.

Security

NSPRI is responsible for the data that it collects and processes and members of staff must take on equitable security measures to protect it by preserving the confidentiality of the data against unsanctioned disclosure or use, upholding the integrity of the data by preventing unauthorized alteration, and allowing only authorized access. All members of staff are individually responsible and liable for assessing the risks arising from a particular processing action and making sure that sound security measures are in place.

- Suitable security measures which are proportionate and responsive to any identified risks in data protection impact assessment (under responsibility above) must be in place at all times.
- All implemented security measures should be periodically revised and, as required, updated by concerned members of staff.
- The use of ICT resources for the handling or storage of data that falls within the scope of this Policy must be managed in compliance with extant Institute guidelines
- Data must be stored in suitable locations and in a mode that protects it from inadvertent or unauthorized processing, loss, theft or corruption.
- Access to the data may only be sanctioned and granted to those who have a need to know in order to fulfil the processing objective. A register of authorized persons and the access rights they have been granted must be kept.
- Before transferring data to third parties for processing, concerned members of staff must confirm that the third parties' security protocols are equivalent to those put in place by NSPRI for that same data.

Transparency

Transparency implies clarity and openness with data providers at the time of collection in terms of "what" data NSPRI intends to collect and process, "why" the processing is necessary, and "how" the data will be processed. The nature of the data and the operational context will determine the level of information to be provided. It is the duty of concerned members of staff to provide the data provider with adequate, pertinent and current information about the processing of their data, including the possibilities for data providers making requests related to their data.

- Concerned members of staff must inform the data provider about the processing of their data throughout the data lifecycle using appropriate notices.
- The whys and wherefores for not providing information must be fully documented and periodically revised to confirm that the conditions upon which the decision to not provide information is predicated have not changed.

Data Classification and Levels of Confidentiality

Data is defined as facts and statistics collected for reference or analysis. It can also be defined as facts, numbers, information that has been translated into a form that is efficient for movement or processing used to analyse or make decisions. Data classification and levels of confidentiality in NSPRI play a crucial role in safeguarding information. The classification comprises four levels:

1. Public Data:
    - Description: Non-sensitive data approved for public dissemination by NSPRI.
    - Risks: None.
    - Examples: Published reports, statistics, press releases, publicly accessible databases on stored products
2. Internal Data:
    - Description: Data requiring internal approval, with moderate associated risks.
    - Risks: Medium.
    - Examples: Internal communications, project documents, draft technical documents, meeting minutes with ongoing project updates, research proposals in the internal review stage, and collaborative work documents within NSPRI teams/programmes.
3. Confidential Data:
    - Description: Sensitive data with high risks if inappropriately disclosed.
    - Risks: High.
    - Examples: Personal data, information on technical assistance, patents, lists of training event attendees, detailed financial reports for specific projects, preliminary findings from proprietary research, Information on experimental methodologies.
4. Strictly/Highly Confidential Data:
    - Description: Highly sensitive data with very high risks if disclosed improperly.
    - Risks: Very high.
    - Examples: Personal data posing serious harm, documents on investigatory proceedings, procurement-related documents with commercially sensitive information, unpublished research with potential commercial applications, Detailed personnel records with sensitive information, and Exclusive agreements with external partners.

Guidelines for NSPRI personnel:

- Release of data must follow established authorization or publication procedures.
- Security measures must be proportionate to the identified confidentiality level.
- Adherence to the confidentiality level set by the data provider before transferring data to NSPRI.
- Regular review and adjustment of data classification to ensure appropriate protection.
- Consultation with relevant authorities in case of doubt or uncertainty regarding confidentiality levels.

This comprehensive framework ensures a robust approach to data protection and confidentiality at NSPRI, aligning with international best practices.

Data Confidentiality

Data confidentiality in NSPRI is a paramount commitment, aligning with stringent ethical standards and international civil service regulations. Key principles guiding data confidentiality include:

1. Duty of Confidentiality:
    - Personnel are bound by the duty of confidentiality, as stipulated in Public Service Rules, Condition of Service, and the Code of Ethical Conduct.

- Applicability extends to all NSPRI personnel, with non-compliance subject to potential disciplinary or administrative action.

2. Data Handling Accountability:
    - Personnel are accountable throughout the data lifecycle, particularly when collecting, processing, and transferring data to third parties.
    - Utmost discretion is mandatory, with a duty to safeguard internal, confidential, or sensitive information acquired through official functions.
3. Confidentiality Assurance:
    - Personnel must ensure the confidentiality of collected, accessed, or processed data.
    - Data access or transfer is permissible solely for the intended processing purpose, and disclosure to any unauthorized party, including third parties or other NSPRI personnel, is strictly prohibited.
4. Authorization Requirement:
    - Explicit authorization is a prerequisite for data access or receipt by any party.
    - Authorized recipients must adhere to security measures commensurate with the level of data confidentiality.

This robust framework ensures that NSPRI personnel adhere to the highest standards of data confidentiality, promoting integrity and trust in handling internal, confidential, or sensitive information.

Application of Data Protection Principle and Confidentiality

Provision of information to data providers

Before data can be collected from the data provider, proper information on what to be done with the data provided such as reasons for data collection, purpose of the data to be collected, if the data will be transferred to a third party, access request, verification, rectification, deletion, or object to the use of their data, complaint, and identity of NSPRI personnel for data related queries/request.

Where personal data is processed, the information provided must be in clear and unambiguous language, appropriate to the age, literacy, and the data provider vulnerability.

Processing of sensitive data

In data processing a specific measure needs to be put in place to ensure proper protection of sensitive data. Prior to data collection, personnel must explore possibility of achieving the processing purpose without processing sensitive data.

Processing of data must be part of NSPRI activities, its mandate and in line with its legal framework. Additionally, personnel may only process sensitive data based on consent of the data provider or protection of the data provider interest.

When processing sensitive data that is likely to result in high risk to data providers and NSPRI, guidance should be sought as regards the appropriate action.

Data transfers

Data received by NSPRI: Personnel must ensure the data received from the provider is being transferred to NSPRI on an appropriate and legitimate basis.

Data transferred by NSPRI to a third party: Personnel must only transfer data to a third party based on the third-party level of protection appropriate to NSPRI's own rules and regulations, and this data policy.

Assessment of protection afforded by a third party: Personnel must ensure that data transferred to third party based on confidentiality must assess a level of protection afforded by the third party, third party's technical and organizational security safeguards, the risks associated with the transfer, and any other relevant transfer element. If the third party cannot afford a level of data protection and privacy as applied by NSPRI, measures to mitigate potential risks must be identified, or the data must not be transferred.

Contractual arrangements: Written data transfer arrangement should be done by incorporating relevant contractual arrangements to the applicable rules for each type of arrangement. In cases where an exception to contractual agreement must be made, protective measures taken must be documented.

Means of Transfer: Data transfer method must ensure its adequate protection during transfer. The level of data confidentiality will determine the means of transfer. Personnel must ensure that the third party will destroy or return to NSPRI all the data transferred once the data achieve its purpose.

Requests by data providers

Type of Requests.

- Data provider must be able to know if their data is being processed and request for access.
- Data provider may request for correction of their data being processed by NSPRI.
- Data provider may request for deletion of their data if there is no need for further processing; withdraw their consent on the data provided; and there exists no legitimate basis for processing by NSPRI.
- Data provider may object to data collection and processing at the collection point. NSPRI personnel must inform the data provider the consequences of data objection as appropriate.

Personnel shall ensure that requests for access, correction, deletion, and objection are received, recorded, validated, handled, and responded to in a timely and efficient manner. If legitimate grounds exist for satisfying a request, personnel must take appropriate action to fully or partially accommodate the request received.

Restrictions.

Data providers may be rejected or restricted if security and safety of personnel, third parties or data providers is or would be compromised; if it contravenes the rules and related directives on confidentiality and information disclosure, and this data privacy and protection policy; and or if the request is unclear or unreasonable.

Data breaches.

Immediately NSPRI personnel become aware of a data breach, personnel must contact NSPRI executive management as appropriate. A determination must be made as to whether the data breach results in risk to the data provider or to NSPRI. The identified risk shall be evaluated and subjected to mitigatory action.

When the data breach results in a risk to the data provider, such breach will be communicated to the data provider as well as the measures implemented to mitigate the risk, unless the communication is deemed unnecessary or inappropriate.

4. Scope and Application

NSPRI as a legal entity is a parastatal under the supervision of ARCN in the Federal Ministry of Agriculture and Food Security. NSPRI enjoys the privilege and access to public information that can be used for research and developmental purpose. This policy establishes the central principles and rules that govern NSPRI's collection, processing, and protection of data.

It sets the minimum standards for protecting data generated by NSPRI or entrusted to NSPRI or any of her representative by a legal person or an individual and forms the basis for internal procedures to manage the application of the Data protection Principles and to monitor continued suitability of the Policy.

This Policy applies to all activities and operations involving the processing of data by NSPRI and by third parties in their relations with NSPRI. All NSPRI personnel must process data in accordance with this Policy. All other internal guidelines and policies addressing specific aspects of data protection must be implemented and interpreted in accordance with this Policy. In the case of any inconsistency, this Policy will prevail. However, This Policy does not apply to public data nor data from anonymous sources.

5. Definition of terms

Anonymized data: refers to information that cannot be used to identify or trace a natural person, or to personal information that has been made anonymous such that the source of the information cannot be recognized.
Consent: is defined as the agreement by data provider as to clear expression of their permission to the processing of their data by NSPRI. This consent might be implicit or, in the case of sensitive data, or explicit in other cases.
Data: is any information that comes from within NSPRI or is elicited by NSPRI from a data provider that is appropriate for processing. Both personal and non-personal data, in any format, are considered data for the purposes of this policy.
Data breach: is a situation which occurs when sensitive data is unintentionally lost, destroyed, altered, accessed, acquired, or used for other unauthorized purposes. This affects the integrity, confidentiality, availability, or security of the data.
Data lifecycle: refers to all stages of the data life cycle, including planning, gathering, processing, storing, transferring, and disposal.
Data provider: is any legal entity or individual who discloses data to NSPRI. Legal entities may disclose an individual's personal data to NSPRI under the terms of this policy, including NSPRI Staff, ARCN and FMAFS organizations, intergovernmental organizations (IGOs), non-governmental organizations (NGOs), and private sector companies.
Data encryption: is the process of transforming data by NSPRI such that it cannot be read without authorized access information, like a "key" or password.
Non- Personal Data: Any financial, technological, or operational data that is unrelated to a named or identifiable individual. Financial reports, a vendor's commercially sensitive data, or material containing security-critical information revealed by members are a few examples of non-personal data.
Personal Data: Any information pertaining to a specific, identifiable person by NSPRI staff. Such as Names, Next of kin, work and home addresses, email addresses, dates of birth, and job titles, are a few examples.
Personnel: refers to employees and affiliates that NSPRI has hired, such as researchers, technologist, consultants, national project personnel, volunteers, interns, and any other people who work for NSPRI on a contractual arrangement.
Processing: is an action or sequence of actions taken by NSPRI on a data, which sometimes is automated or not, in order to establish a fact. These actions include gathering, logging, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, transferring (whether orally, in writing, or on a computer), disseminating, or otherwise making the data available, as well as correction or destruction.
Pseudonymization: is the processing of data such that it can no longer be traced back to a particular data provider without the use of additional information. Such supplementary data needs to be maintained independently and is protected by technological safeguards to prevent personal information from being linked to a specific person.

Sensitive data: is any information that staff members have deemed to be sensitive based on the possibility and significance of potential dangers that could arise from their improper disclosure. This includes but is not limited to personal information that discloses an individual's racial or ethnic origin, political ideas, religious beliefs, genetic information, or biometric information, all of which are automatically deemed to be extremely sensitive information. It also includes non-personal information that is relevant to national security, commercially or economically sensitive, or that is otherwise similarly sensitive and supplied by NSPRI employees or other authorized individuals.

Third party: Any organization to which data is transferred, excluding NSPRI and the data provider.
Contractual agreement: is a legally binding agreement between two parties. The contract's terms and conditions will require the parties to either do or refrain from doing specific actions.

Data protection/Security: - also known as data privacy or information privacy refers specifically to measures taken to protect the integrity of the data itself against manipulations and malware. It provides defence from internal and external threats and safeguards information from loss through backup and recovery.

Data privacy refers to controlling access to data.

Types of data protection.

1. Encryption
2. Backup and recovery
3. Access control
4. Network security
5. Physical Security
6. Data masking
7. Data resiliency
8. Data erasure
9. Hardware security.
10. Software security

Data privacy is about keeping your information from being sold or shared, while data protection focuses on keeping that information from hackers. E.g. Names, addresses, emails, Telephone numbers and bank or credit card details.

6. Responsibilities and Oversight

The Oversight Advisory Committee

The data protection and policy-making committee, by its defined terms of reference, is responsible for ensuring that the current Policy is implemented effectively and efficiently. This committee operates with complete autonomy and exercises independent oversight to ensure that the Policy is being executed in a manner that aligns with the NSPRI rules and regulations. Through its rigorous oversight, the committee ensures that any deviations from the Policy are identified and addressed promptly, thereby safeguarding the integrity of the Policy and the Institute as a whole.

7. Procedure to ensure compliance.

Data Protection and Policy Oversight Committee

The Committee is entrusted with the responsibility of overseeing the comprehensive array of data protection activities within NSPRI. As a crucial aspect of its mandate, it closely monitors the implementation of the prevailing Data Protection Policy. The Committee is directly accountable to the Executive Director and reports to this office regularly. Its also serves as a primary advisory body to the Director concerning various data protection matters. Through an unwavering commitment to its core objectives, the Committee endeavours to ensure that members of staff adhere to the highest standards of data protection and privacy practices.

The Data Protection Oversight Committee is comprised of:

a) Chairman: 1 person

b) Members: 6

The oversight of data protection activities and security officers across the Institute is entrusted to the Policy-Making Committee. This committee diligently monitors the implementation of policies, recommends their

development, and receives regular reports. Additionally, it conducts a review of the policy every four (4) years, reports its findings to the Executive Director, and ensures that the Policy is aligned with institutional strategies. The Committee must hold at least two (2) meetings annually, which may be held virtually or in person. Decisions may be made via correspondence upon mutual agreement among the committee members.

8. Compliance

Personnel

All personnel must comply with this Policy and related instruments. The following are the specific responsibilities of personnel:

a) Determine the purposes and means of implementing the policy without compromising the existing data by the present Policy. Personnel should consider the kinds of data that the policy covers and how it should be processed and ensure that it does not breach any laws or regulations.

b) Implement appropriate technical and organizational measures to ensure that data processing is carried out following this Policy. This may include the conclusion of appropriate contractual instruments. Personnel should periodically review and update these measures where necessary to ensure their effectiveness.

c) Keep appropriate records of data processing operations, data sharing agreements, requests and complaints by data providers, data protection impact assessments, data breach notifications, requests by data providers, and related matters. Records should be accurate, up-to-date, and must be available for inspection by authorized personnel.

d) Immediately inform their supervisors in case of data breaches. Personnel should also cooperate in any investigation of a suspected data breach.

9. Review/Revision and Amendment

- This policy will be reviewed by the Data Protection Policy Committee or any designated Committee a year after its validation and duly corrected as deemed necessary. Subsequently, it will be reviewed in consultation with Internal Management Committee, at least in (2) years with the perspective to ensure the intention has not been defective, and to comply with updated requirements to the Institute's operations in protecting all classification of data, building stakeholders' trust, and good reputation.

- Amendments to this Policy shall take effect immediately after it is published.

Effective Date

- The policy takes effect on the date of publication and becomes an edict protecting all classification of data in the Institute, until otherwise stated.

11. Additional Information

The Forms of Data in Nigerian Stored Product Research Institute (NSPRI)

1. Data on Staff Records. Eg. Nominal roll, Variation advice, Personnel files etc
2. Financial Data. Eg. Payment Vouchers, staff pay slips, Bank Statement etc
3. Stakeholder's records/Demography.
4. Data on Technology
5. Research Data
6. Information Data (Digitalized, Electronic software.)