





Healthy Shield
FOUNDATION

DATA PROTECTION POLICY

2022

DATA PROTECTION POLICY

Revision Timeline	Two years after approval
Policy owner	Healthy Shield Foundation (HESHIF)
Status	Not for profit

Date Issued	August 01, 2022	
Approved by	Monica Pili Bernard Chief Executive Officer Healthy Shield Foundation (HESHIF)	August 01, 2022 
Endorsed by	Adv. Walta Carlos Chair Person, Board of Directors, Healthy Shield Foundation (HESHIF)	August 01, 2022 



1



Contents

Introduction	1
Art 1. Aim of the HESHIF Data Protection Policy	1
Art 2. Scope	2
Art 3. Definitions	2
Art 4. Factual accuracy and up-to-datedness of data	3
Art 5. Data processing principles	3
Art 6. Data protection management	4
Art 7. Data processing Compliance	5
Art 8. Confidentiality of data processing	6
Art 9. Minimization of data collection	6
Art 10. Safeguarding and security of data	7
Art 11. Processing data relating to a child	7
Art 12. Data protection impact assessment	7
Art 13. Processing of sensitive personal data	7
Art 14. Transmission of personal data	8
Art 15. Onward reporting	8
Art 16. Training and awareness	9
Art 17. Roles and responsibilities	9
Art 18. Independent assurance	9
Art 19. Data retention	9
Art 20. Data preservation timeline	9
Art 21. Data deletion	10
Article 22. Policy review	10
Related policies	10



2



Introduction

Recent concerns about the security of personal data stored in institutions have led to Governments enacting data protection regulations. In 2018 the European Union (EU) operationalized the General Data Protection Regulations (GDPR) that governs how companies handle personal data. Consequently, in Tanzanian law on data protection is still embryonic as there is not yet a comprehensive legislation on this area, although it is understood that a draft National Data Protection Bill ('the Draft Bill') is on the horizon and will soon be unveiled. Therefore, whatever data protection provisions there are, they are to be found to varying degrees in a number of legislations, especially from the banking, electronic, and telecommunications sectors, as well as penal statutes. In particular, the nature of such provisions have generally been focused on protecting confidentiality and privacy, without any detailed provisions on how data is to be collected, maintained, and handled.

HESHIF is committed to comply with all relevant Tanzanian legislation and applicable global legislations related to data protection; recognizes that the protection of individuals through lawful, legitimate, and responsible processing and use of their personal data is a fundamental human right.

HESHIF will ensure that it protects the rights of data subjects and that the data it collects and processes comply with national and global standards required by the legislation.

Art 1. Aim of the HESHIF Data Protection Policy

HESHIF acknowledges that information technology should be at the service of every citizen, and that information technology development shall take place in the context of national and international cooperation. Information technology shall not violate human identity, human rights, privacy, or individual or public liberties. HESHIF is committed to national, regional and international compliance with data protection laws.

This data protection policy provides guidance on how HESHIF will handle the data it collects. It helps HESHIF to comply with the data protection law, protect the rights of the data subjects and protects from risks related to breaches of data protection. It applies regionally to HESHIF and is based on globally accepted basic principles on data protection. Ensuring data protection is the foundation of trustworthy relationships and the reputation of HESHIF as a credible organisation.

The HESHIF Data Protection Policy ensures the adequate level of data protection as prescribed by the current Tanzanian relevant legal frameworks, including in countries that do not yet have adequate data protection laws.

It is meant to be a practical and easy to understand document to which all HESHIF departments, stakeholders and partners can refer to.

Art 2. Scope

This Data Protection Policy applies to all entities of HESHIF, including network and implementing partner organizations in all countries of operation.

The policy applies to:

- HESHIF staff and board members who handle and use the organisation's information (where HESHIF is the 'Controller' for the personal data being processed, be it in manual and automated forms.
- Any person employed by an entity that carries out missions for HESHIF; In particular, the implementing partners, suppliers, sub-grantees, stakeholders and other associated entities.
- All personal data processing HESHIF carries out for others (where HESHIF is the 'Processor' for the personal data being processed) and,
- All formats, e.g., printed and digital information, text and images, documents and records, data and audio recordings.

Art 3. Definitions

- **Data controller**, means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of the processing of personal data; adapted from the Tanzanian Data Protection Bill.
- **Data processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.
- **Data subject** means an identified or identifiable natural person who is the subject of personal data.
- **Personal data** means any information relating to an identified or identifiable natural person.
- **A personal data breach** means 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.
- **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.
- **Processing data** means any operation or sets of operations performed on personal data whether or not by automated means, such as:



- Collection, recording, organization, structuring;
- Storage, adaptation or alteration;
- Retrieval, consultation or use;
- Disclosure by transmission, dissemination, or otherwise making available; or
- Alignment or combination, restriction, erasure or destruction

Art 4. Factual accuracy and up-to-datedness of data

Personal data on file must be correct, complete, and – if necessary – kept up to date. Suitable steps must be taken to ensure that inaccurate or incomplete data are deleted, corrected, supplemented or updated.

Art 5. Data processing principles

Data processing at HESHIF adhere to the following principles:

1. Fairness and lawfulness

When processing personal data, the individual rights of the data subjects must be protected.

HESHIF will ensure that personal data is:

- Processed lawfully, fairly, in a transparent manner and in line with the right to privacy.
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is to be processed.
- Collected only for specified, explicit and legitimate purposes and shall not subsequently be processed in a manner that is incompatible with those purposes.
- Processed in a manner that ensures its security using appropriate technical and organizational measures to protect against unauthorized or unlawful processing and accidental loss, destruction, or damage.
- Processed upon voluntary consent of the person concerned.

2. Restriction to a specific purpose

Processing of personal data shall:

- Not be excessive in relation to the purposes for which they are obtained and their further processing.
- Be accurate and where necessary kept up to date.
- Not keep data in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed.



- Be processed only for the purpose that was defined before the data was collected.
- Not transfer data out of Tanzania unless there is proof of adequate data safeguards/ measures or consent from the data subject.
- However, further data processing for statistical, scientific and historical purposes shall be considered compatible with the initial purposes of the data collection, if it is not used to make decisions with respect to the data subjects.

3. Transparency

In general, personal data must be collected directly from the individual concerned

- The data subject must be informed of how his/her data is being handled.
- When the data is collected, the data subject must either be made aware of, or informed of: - the purpose of data processing; - Categories of third parties to whom the data might be transmitted
- Processing of personal data must have received the consent of the data subject or must meet one of the following conditions: - compliance with any legal obligation to which HESHIF is subject; - the protection of the data subject's privacy; and - the performance of a service mission entrusted to HESHIF

4. Confidentiality and data security

- Personal data is subject to data secrecy.
- It must be treated as confidential on a personal level and secured with suitable organisational and technical measures to prevent unauthorised access, illegal processing or distribution, as well as accidental loss, modification or destruction.

Art 6. Data protection management

HESHIF has designated the Communications Officer to be the Data Protection Manager (DPM). Accordingly, the DPM will:

- Advise HESHIF staff on requirements for data protection, including data protection impact assessments.
- Ensure that HESHIF has complied with the legal requirements on data protection.
- Facilitate capacity building of staff involved in data processing operations.
- Cooperate with external regulators on matters relating to data protection.



4



Art 7. Data processing Compliance

HESHIF has a duty to notify data subjects of their rights before processing data.

1. Consent to Data Processing

- Individual data can be processed upon consent of the person concerned.
- Declarations of consent must be submitted voluntarily.
- In certain exceptional circumstances, consent may be given verbally.
- Where necessary, HESHIF will maintain adequate records to show that consent was obtained before processing personal data.
- No data will be processed after the withdrawal of consent by the data subject.

2. Telecommunications and Internet

- Telephone equipment, e-mail addresses, intranet and internet along with internal social networks are provided by HESHIF primarily for work-related assignments. They are a tool and an organisational resource. They can be used within the applicable legal regulations and internal HESHIF communication policies. In the event of authorised use for private purposes, the laws on secrecy of telecommunications and the relevant national telecommunication laws must be observed if applicable.
- There will be no general monitoring of telephone and e-mail communications or intranet/internet use. To defend against attacks on the IT infrastructure or individual users, protective measures can be implemented for the connections to the network used by HESHIF that block technically harmful content or that analyse the attack patterns. For security reasons, the use of telephone equipment, e-mail addresses, the intranet/internet and internal social networks can be blocked for a temporary period. Evaluations of this data from a specific person can be made only in a concrete, justified case of suspected violations of policies and/or procedures of HESHIF. The evaluations can be conducted only by investigating departments while ensuring that the principle of proportionality is met. The relevant national laws must be observed in the same manner as the HESHIF regulations.

3. The Rights of the data subjects

All individuals who are the subject of personal data held by HESHIF are entitled:

- To be informed of the use to which their personal data is to be put.
- To object to the processing of all or part of their personal data.
- To the correction of false or misleading data.
- To delete false or misleading data about them.



5



- To request information on which personal data relating to him/her has been stored, how the data was collected, and for what intended purpose. If there are further rights to view the employer's documents (e.g. personnel file) for the employment relationship under the relevant employment laws, these will remain unaffected. If personal data is transmitted to third parties, individuals should be informed of such a possibility. If personal data is incorrect or incomplete, the data subject can demand that it be corrected or supplemented.
- To request his/her data to be deleted if the processing of such data has no legal basis, or if the legal basis has ceased to apply. The same applies if the purpose behind the data processing has lapsed or ceased to be applicable for other reasons. Existing retention periods and conflicting interests meriting protection must be observed.
- To object to his/her data being processed, and this must be taken into account if the protection of his/her interests takes precedence over the interest of the data controller owing to a particular personal situation. This does not apply if a legal provision requires the data to be processed.

Art 8. Confidentiality of data processing

Personal data is subject to data secrecy. Any unauthorised collection, processing, or use of such data by employees is prohibited. Any data processing undertaken by an employee that he/she has not been authorised to carry out as part of his/her legitimate duties is unauthorised. The "need to know" principle applies. Duly-authorized employees may have access to personal information only as is appropriate for the type and scope of the task in question. This requires a careful breakdown and separation, as well as implementation, of roles and responsibilities. Employees are forbidden to use personal data for private or commercial purposes, to disclose it to unauthorised persons, or to make it available in any other way. Supervisors must inform their employees at the start of the employment relationship about the obligation to protect data secrecy. This obligation shall remain in force even after employment has ended.

Art 9. Minimization of data collection

Data must only be collected for the performance of duties and tasks; staff must not ask data subjects to provide personal data unless that is strictly necessary for the intended purpose.

Staff must ensure that they delete, destroy, or anonymise any personal data that is no longer needed for the specific purpose for which they were collected.



Art 10. Safeguarding and security of data

HESHIF has instituted data security measures which are laid out in safeguarding policy and Operational hand book. These measures serve to safeguard personal data and must be complied with accordingly.

Art 11. Processing data relating to a child

HESHIF will not process data relating to a child unless consent is given by the child's guardian or parent and the processing is in such a manner that protects and advances the rights and best interests of the child in line with HESHIF Safeguarding policy.

HESHIF will institute adequate mechanisms to verify the age and obtain consent before processing the data.

Art 12. Data protection impact assessment

HESHIF will undertake a data protection impact assessment whenever they identify that the processing operation will likely result in a high risk to the rights and freedoms of any data subject. The data protection impact assessment will be done before processing the data. It is the responsibility of the DPM to carry out the impact assessment.

Art 13. Processing of sensitive personal data

HESHIF will process sensitive personal data only when:

The processing is carried out in the course of legitimate activities with appropriate safeguards and that the processing relates solely to the staff or to persons who have regular contact with HESHIF, and the personal data is not disclosed outside the organisation without the consent of the data subject.

The processing relates to personal data that has been made public by the data subject. Processing is necessary for:

- The establishment, exercise or defense of a legal claim.
- The purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject.
- Protecting the vital interests of the data subject or another person where the data subject is physically or legally incapable of giving consent.



7



Art 14. Transmission of personal data

- Transmission of personal data to recipients outside or inside HESHIF is subject to the authorisation requirements for processing personal data under Section 7 and requires the consent of the data subject.
- The data recipient must be required to use the data only for the defined purposes.
- In the event that data is transmitted to a recipient outside HESHIF, this recipient must agree to maintain a data protection level equivalent to this Data Protection Policy. This does not apply if transmission is based on a legal obligation.
- Generally, no personal data shall be transmitted out of Tanzania without the consent of data subject; and
- The transfer of data will be only when there is proof of appropriate measures for security and protection of the personal data, and the proof provided to the Data Protection Commissioner in accordance with Tanzania's related Data Protection legislations i.e. Cyber Crimes Act of 2015.

However, the transfer is necessary for the performance of a contract, implementation of pre-contractual measures such as:

- For the conclusion or performance of a contract to which the data subject is part of.
- For matter of public interest
- For legal claims.
- To protect the vital interests of data subjects.
- To fulfill donor requirement(s)- (proof of implemented project activities.)
- For compelling legitimate interests pursued by the data controller or data processor which are not overridden by the interests, rights and freedoms of the data subjects.

HESHIF will process sensitive personal data out of Tanzania only after obtaining the consent of a data subject and on receiving confirmation of appropriate safeguards.

Art 15. Onward reporting

In line with regulatory requirements, HESHIF will report to the Data Protection Commissioner any data breach within 72 hours of being aware.

HESHIF will also communicate the data breach to the data subject as soon as is practical unless the identity of the data subject cannot be established.

Art 16. Training and awareness

HESHIF will train staff on the contents and implementation of this policy. Staffs joining HESHIF will be required to go through an induction process that entails familiarization with this policy.

HESHIF will ensure that the requirements of this policy form part of its agreement with its grantees, and third parties who process HESHIF data.

Art 17. Roles and responsibilities

All staff must play the following roles and responsibilities:

- Report suspicions of breaches promptly;
- Read, understand and comply with the contents of this policy;
- All project leads and managers must ensure staff and third parties they work with are aware of the contents of this policy; and
- Conduct risk assessments, and update controls and procedures to mitigate the risk of data breaches.

The Chief Executive Officer (CEO) and Program Manager are responsible for ensuring employees are aware of the policy and are supported to implement and work by it, as well as creating a management culture that encourages a focus on data protection.

Art 18. Independent assurance

The adequacy and effectiveness of HESHIF data protection procedures is subject to the regular internal audit reviews where necessary HESHIF may call an external review to provide assurance over the integrity.

Art 19. Data retention

The Data retention period in HESHIF is determined by legitimate needs. Adequate records of decision making will be maintained to show cause.

Art 20. Data preservation timeline

The Data will be retained by HESHIF for at least a period of ten (10) years. After this time the data may be subject to deletion; if it has not been reused, accessed, or cited.



9



Art 21. Data deletion

Personal data shall be retained in a form that allows the identification of the data subjects for a period no longer than is necessary for the purposes for which they are obtained and processed. There may be an indication of interests that merit protection or historical significance of this data in individual cases. If so, the data must remain on file until the interests that merit protection have been clarified legally, or the corporate archive has evaluated the data to determine whether it must be retained for historical purposes.


Article 22. Policy review

The Program Manager is responsible for ensuring that this policy is reviewed on a timely basis. This policy will be reviewed after every two years accordingly as approved by the board.


Related policies

This policy should be read in conjunction with:

- Anti-Sexual Harassment Policy
- Anti-bribery/corruption Policy
- Conflict of Interest Policy
- Child & Young people safeguarding policy
- Code of Conduct in the Operation Handbook

Approval Status:	APPROVED
BOARD MEMBERS	
Name	Signature
WALTA JULIUS CARLOS	



STAFF MEMBERS	
MONICA PILI BERNARD	
MILAH JOSEPH	
CONSULTANTS	

