POLICY NUMBER: CS/POL/302

ORGANISATION: FSD AFRICA

TITLE: DATA PROTECTION POLICY

EFFECTIVE DATE: ----JULY 2021

VERSION: 2023 NOVEMBER

Policy Summary

Title	**Data Protection Policy**	
Version	October 2023	
Confidentiality	Internal	
Owner	Director Corporate Services	
Review date	November 2023	
Frequency of review	After two years of operation, every two years subsequently	
Background	FSD Africa strives to ensure that all of its activities in relation to the record keeping, storage, and security of data are conducted to the highest ethical standards and in compliance with its legal obligations. During the course of FSD Africa's activities it will collect, store and process personal data about its funders, its investment counterparties, recipients of funding and their customers, suppliers and employees. FSD Africa recognises that the correct and lawful treatment of such data will maintain confidence in the organisation and will provide for successful operations.	
Related policies	▪ Code of Conduct ▪ The IT Policy ▪ Disciplinary Policy	
Policy Reviewers	Director Corporate Services	Type equation here.
	EXCO	Type equation here.
	Chief Financial Officer/ Director Corporate Services	Type equation here.
	Staff Consultative Committee Representative	Type equation here.
Policy Approvers	Director HR and Talent Management	Type equation here.
	CEO	Type equation here.
	NRC Chair	Type equation here.
	Legal	Type equation here.

What has changed in the current version	This is a revised Policy to align with the new legislation, Kenya Data Protection Act 2019 as well as other best practices The proposed email address is for the Data Protection Officer to manage data breaches - dataprotection@fsdafrica.org.

Contents

1. Introduction

Data protection has increasingly become a sensitive and business critical consideration in all organisations. The usage, storage and sharing of data in an increasingly connected cyberspace now requires stringent governance to ensure that data is only shared with the intended recipients and is only kept for the duration that is acceptable and compliant with business ethics and standards.

This Data Protection Policy describes the types of personal information FSD Africa and its subsidiary FSD Africa (Investments) Limited (together **FSD Africa**) obtains, how it is used, with whom it may be shared and the measures taken to safeguard the information so obtained.

2. Regulatory standards

Ensuring data protection and privacy is a requirement of several regulatory standards. These include:

a) Kenya Data Protection Act 2019 (the **Act**)
b) The Constitution of Kenya 2010
c) The EU General Data Protection Regulations, 2018

3. Contextual overview of the Act

a) The Act came into force in 2019 to operationalise the right to privacy under Kenya's Constitution. The development of privacy law through the Act is incremental, and the evolution of the standards it has introduced is expected through the issuance of guidelines, codes of practice, and regulations over time. New changes will be incorporated into the Policy at every biennial review.

b) With the Act in force, clear obligations have been delineated with respect to the observance of the right to privacy. FSD Africa handles personal data belonging to natural persons who are located in Kenya. These include its employees, and the individuals who work for its vendors, third party contractors, donors, and grant recipients. The personal data which FSD Africa collects and processes includes names, biographical data, contact details, physical and email addresses, bank account numbers, next of kin details, taxpayer registration numbers, and photographs, among others.

c) Within these relationships, FSD Africa is a Data Controller under the Act given it determines the purpose and means of processing the personal data it collects in respect of these individuals. It is thus obligated to comply with the principles of data processing provided in the Act. Its employees, and the individuals associated with its vendors, third party contractors, donors, and grant recipients in this context are the data subjects.

d) Among FSD Africa's obligations under the Act is to put in place a data protection policy. This policy is issued pursuant to that obligation.

4. Policy statement

FSD Africa recognise how critical and sensitive private data is. FSD Africa will, therefore, strive to ensure that it respects and protects all data in its possession with utmost care in line with the applicable legislation.

5. Purpose of the policy

This Policy seeks to ensure compliance with the Act with respect to the gathering, recording, storing, retrieval, consultation, use, disclosure, processing and transferring of personal data whether that data is held on a computerised system or manually (including emails).

This Policy further recognises that not all pillars within FSD Africa are the same and that data is used differently by each. The principles of productivity apply to this Policy and without any limit or restriction to these principles.

6. Definitions

Data subject - an identified or identifiable natural person about whom FSD Africa holds personal data.

Data processor – means a natural or legal person, public authority, agency, or other body who processes personal data on behalf of a data controller.

Personal data - data relating to an individual who can be identified from that data (or from that data or other information in FSD Africa's possession). Personal data can be factual (for example a name, address or date of birth) or it can be an opinion about a person or their actions or behaviour.

Personal Data Breach - a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Processing - any activity that involves the use of personal data. It includes obtaining, recording, or holding the data or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also refers to transferring personal data to third parties.

Sensitive personal data - includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life or about the commissioning of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of the court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

Confidential or Proprietary Information - any secret, confidential or proprietary information of FSD Africa, or any secret, confidential or proprietary information entrusted to FSD Africa by any other person or entity.

Data controller - a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of the processing of personal data.

7. Scope of the policy

This Policy applies to: all Board members, committee members and advisors, employees, contractors, casuals, interns, job applicants, donors, and grant recipients of FSD Africa. .

However, the scenarios below may require special attention in terms of disclosure requirements:

a) If required or permitted to do so by applicable law, regulation or legal process such as a court order.
b) To law enforcement authorities or other government officials to comply with a legitimate legal request.
c) When FSD Africa believes disclosure is necessary to prevent physical harm or financial loss to the organisation or the public as required or permitted by law.
d) In connection with an investigation of suspected or actual fraud, illegal activity, security or technical issues.

8. Data protection principles

FSD Africa will:

a) Ensure personal data is processed in accordance with the right to privacy as conferred in the Constitution of Kenya, 2010.
b) Ensure confidentiality, that is, information is accessible only to authorised individuals.
c) Protect integrity, namely that information is accurate and complete. FSD Africa will take measures to ensure the integrity of data /information.
d) Process personal data fairly and in accordance with, and on the basis of, applicable law. This will require, among other things:
    i. the data subject's consent to the processing, or
    ii. the processing is necessary for the performance of a contract with the data subject, or
    iii. the processing is in compliance with a legal obligation to which FSD Africa is subject, or
    iv. The processing is required for the legitimate interest of FSD Africa or the party to whom the relevant data is disclosed.

When sensitive personal data is being processed, additional conditions as provided by the IT Department must be met.

e) Ensure availability, that is, authorised users have access to the information they need to carry out their tasks/roles.
f) Ensure personal data obtained from data subjects is processed in accordance with the purpose in which it was collected for.

9. Data management

a) Prior to collecting personal data, FSD Africa will notify data subjects of the following:
    i. their right to:
        a. be informed of the use to which their personal data will be put;
        b. to access their personal data;
        c. to object to the processing of their personal data;
        d. to not be subjected to automated individual decision making;
        e. to have their personal data made available in a form that is easy to transfer to a different data controller or data processor;
        f. to the correction of false or misleading personal data about them; and
        g. to the deletion of false or misleading personal data.

ii. the fact that personal data is being collected;
iii. the third parties to whom their personal data might be transferred to, including their contacts;
iv. a description of the technical and organisational security measures that FSD Africa has put in place to ensure the integrity and confidentiality of data that is collected;
v. the basis on which personal data is collected; and
vi. the consequences (if any), where a data subject fails to provide their personal data in whole or in part.

b) FSD Africa will ensure that the personal data they collect is adequate, relevant and limited to what necessary is necessary for the purposes for which it is to be processed. The lawful bases FSD Africa relies on include:

i. performance of the employment contract, such as payment of salaries and conduct of HR functions (disciplinary and grievance mechanisms etc).
ii. to protect the vital interest of the employee, such as provision of medical/insurance cover.
iii. compliance with legal obligations, such as mandatory NHIF and NSSF deductions.
iv. to further a legitimate interest of the employer, such as protection of vital company information as well as monitoring for detection of fraud and illegal activities etc.
v. performance of service contract between FSD Africa and its donors or grant funding recipients.
vi. performance of contract between FSD Africa and its contractors, suppliers or any other third party.

c) Prior to collecting personal data, including sensitive personal data, FSD Africa will, where appropriate, obtain consent from data subjects or disclose the lawful basis relied on where consent is not sought. For example, where personal data must be processed for the performance of a contract, FSD Africa will not seek consent and instead inform the data subjects of the lawful basis relied on.

d) Personal data will only be collected for specified, explicit and legitimate purposes. The data will be processed to the extent that it is required for the specific purpose notified to the data subject.

e) FSD Africa will ensure that personal data that it holds is accurate and kept up to date. It will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. It will also take all reasonable steps to destroy or amend inaccurate or out-of-date data.

f) FSD Africa regularly reviews the personal data in its possession with a view to assessing the need for retention. Personal data shall not be kept in a form that permits identification of data subjects for longer than is necessary for the purpose or purposes for which it was collected. FSD Africa will take reasonable steps to anonymise, destroy, or erase from its systems, all data which is no longer required.

g) All personal data will be processed in line with the following rights of data subjects:

i. to be informed of the use to which their personal data is to be put;
ii. to request access to any data held about them;
iii. to object to the processing of all or part of their personal data;
iv. to ask to have inaccurate data amended; and
v. to not be subjected to automated individual decision making.

10. Data security and protection

a) FSD Africa will take appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. FSD Africa shall maintain data security by protecting the confidentiality, integrity, and availability of personal data

b) In the event of a personal data breach within the meaning of the Act which requires notification, FSD Africa will notify the Data Commissioner within the statutory timelines. FSD Africa will also, where necessary, inform affected data subjects.

c) FSD Africa may transfer any personal data that it holds to another country on any of the following lawful bases:

i. the country to which the personal data is transferred ensures an adequate level of protection for the data subjects' rights and freedoms;
ii. the transfer is reasonably necessary for the performance of a contract between FSD Africa and the data subject, or to protect the interests of the data subject, or is necessary for legitimate interests such as public interest grounds or the establishment, exercise or defence of legal claims;
iii. where FSD Africa has adduced that adequate safeguards otherwise exist with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms and the exercise of their rights; or
iv. the data subject, aware of the risks involved, has consented to the transfer.

d) FSD Africa will only transfer sensitive personal data outside Kenya where the data subject has consented to the transfer, and where there exists appropriate safeguards.

e) FSD Africa commits to protecting its trade secrets, confidential and proprietary information and to ensuring that information and work remain its sole and exclusive property. Consistent with this objective, new employees, as a condition of employment, are required to read and sign a Confidentiality Agreement which forms part of their employment contract, prior to commencing their employment.

f) Personal, privileged and/or confidential information about donors may only be collected, used, disclosed and retained for the purposes identified by FSD Africa as necessary. Employees must therefore ensure that no personal, privileged or confidential donor information is disclosed without the donor's consent and then only if security procedures are satisfied.

g) FSD Africa will use a risk-based approach in data management i.e. risk assessment, information classification, vulnerability assessment and security reviews. It will identify, quantify, and prioritise risks for mitigation.

h) Data privacy and protection controls (e.g. ISO 27001) shall be selected after due consideration of budget and deployment requirements.

i) Personal data relating to a child will not be processed 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 as provided for by the Safeguarding policy.

j) This Policy recognises that not all pillars within FSD Africa are the same and that data is used differently by the various pillars. The principles of productivity apply to this Policy and this document is not intended to limit or restrict the Pillars' productivity. This Policy applies to all areas within FSD Africa.

11. Information classification

a) All FSD Africa information must be classified according to its sensitivity to ensure that appropriate controls are applied during its creation, storage, processing and disposal.

b) The classification criteria is to be used for all information, whether electronically stored, paper based, or intellectually retained.

c) FSD Africa has adopted Data Loss Prevention mechanisms in its systems, to classify sensitive information, alert and inform employees when they are handling sensitive data, and to ensure compliance with listed Data Protection bodies.

The four levels of information classification are as follows:

i. Restricted - This classification applies to the highly sensitive information. Its unauthorised disclosure, use, destruction or modification could cause irreparable/crippling damage to FSD Africa's reputation or brand, its partners and/or Stakeholders, or result in a material financial loss.
ii. Confidential - This classification applies to information which is of such a nature that unauthorised disclosure, use, destruction or modification could cause loss of public respect, or damage to FSD Africa's reputation or brand, its partners and/or stakeholders, or result in a major financial loss. It should be shared on a need-to-know basis.
iii. Internal Use Only - This classification applies to information which is of such a nature that unauthorised disclosure, use, destruction or modification would be against the best interests of FSD Africa, its partners and/or stakeholders. It should be shared only within the confines of FSD Africa domain.
iv. Public - This classification is for information that has been released to the general public, or that requires no protection against disclosure. Such information is not considered sensitive and need not contain any visible evidence of its classification level. This information will typically be shared on the FSD Africa website.

12. Exercising data subjects' rights

Data subjects intending to exercise any of their rights, or to lodge any complaints relating to the processing of their personal data may reach out to the Data Protection Officer designated by Executive Management as set out below in paragraph 13.

13. Responsibilities

a) Executive Management

Executive Management will:

i. Ensure the effective implementation of this Policy and associated Procedures and ensuring that everyone linked with FSD Africa is equipped and supported to meet their responsibilities.

ii. Designate a Data Protection Officer who will be responsible for regulatory compliance, capacity building and play an advisory role to both Management and employees on data protection issues. Additionally, the Data Protection Officer will be in charge of reporting and management of data breaches which will be done through the email address dataprotection@fsdafrica.org.

iii. Ensure that regular data protection impact assessments are done particularly when there is a likelihood of breach of the rights and freedoms of any data subject before processing the data.

b) Board of Directors

The Board has the overall oversight responsibility of this policy and has delegated its implementation to the CEO.

c) IT Team / Security Committee

The IT Team / Security Committee is responsible for coordinating and overseeing company-wide compliance with this Policy and its associated procedure and will review and make recommendations on the security policy framework, architecture and security awareness programs. The requirements of this Policy will be incorporated into FSD Africa's operational procedures and contractual arrangements The IT Team / Security Committee will ensure employees, contractors, consultants and other third parties are made aware of this Policy.

14. Related policies

This Policy should be read in conjunction with:

a) Code of Conduct
b) The IT Policy
c) Disciplinary Policy
d) Online Privacy Policy

15. Review of this policy

The Director, Corporate Services is responsible for updating this Policy and the associated Procedure by using the matrix below and providing some background and context for the revision. The Policy will be approved by the Board.

Policy Title:	**DATA PROTECTION POLICY**		
Policy #	CS/POL/302	Issue Date:	
Review Date		Supersedes Version	
Approver		Previous Version Date	
Approver Title		Next Approval Date	
Policy Clarification			
Title/Office	Telephone	Email /Webpage	
Director Corporate Services			