

Data Protection Policy

Date of revision	Two years after approval
Policy owner	Chief Operating Officer
Status	Public

Version Control

Draft	Submitted		Reviewed	Approved
Version 1	ABC-LLP	4 October	20 October 2020	
Version 2	ABC-LLP	5 November	30 November 2020	10 December 2020

Contents of this policy

1. Introduction	3
2. Policy statement	3
3. Purpose	3
4. Scope	3
5. Definitions.....	3
6. Principles	4
7. Data protection officer	4
8. Duty to notify	5
9. Lawful and fair processing of data.....	5
10. Minimisation of collection	5
11. Accuracy of data	5
12. Safeguards and security of data	6
13. Consent.....	6
14. Processing data relating to a child.....	6
15. Data protection impact assessment	6
16. Processing sensitive personal data.....	6
17. Transferring personal data out of Kenya	7
18. Onward reporting	7
19. Training and awareness	7
20. Grantees or partners	7
21. Roles and responsibilities.....	7
22. Independent assurance	8
23. Data retention.....	8
24. Review of this policy	8
25. Related policies.....	8

1. 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) operationalised the General Data Protection Regulations (GDPR) that govern how companies handle personal data. Consequently, in 2019 Kenya enacted its own Data Protection Act. The regulations seek to protect the privacy of individuals by enforcing responsible processing of personal data. This includes embedding principles of lawful processing, minimising the collection of data, ensuring the accuracy of data and adopting security safeguards to protect personal data.

2. Policy statement

FSD Kenya is committed to complying with all relevant Kenyan legislation and applicable global legislations. FSD Kenya recognises that the protection of individuals through lawful, legitimate, and responsible processing and use of their personal data is a fundamental human right.

FSD Kenya will ensure that it protects the rights of data subjects and that the data it collects, and processes is done in line with the required legislation. FSD Kenya staff must comply with this policy, breach of which could result in disciplinary action.

3. Purpose

The policy provides guidance on how FSD Kenya will handle the data it collects. It helps FSD Kenya comply with the data protection law, protect the rights of the data subjects and protects FSD Kenya from risks related to breaches of data protection.

4. Scope

The policy applies to:

- a) Employees of FSD Kenya and all FSD Kenya's associated parties such as members of the Programme Investment Committee (PIC), Trustees, implementing partners, vendors, contractors and any other third party who handle and use FSD Kenya information (where FSD Kenya is the '**Controller**' for the personal data being processed, be it in manual and automated forms or if others hold it on their systems for FSD Kenya;
- b) All personal data processing FSD Kenya carries out for others (where FSD Kenya is the '**Processor**' for the personal data being processed) and,
- c) All formats, e.g., printed and digital information, text and images, documents and records, data and audio recordings.

5. Definitions¹

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.

¹ Adapted from the Kenya Data Protection Act

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, unauthorised 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 (a) collection, recording, organisation, 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.

6. Principles

FSD Kenya will ensure that data is:

- a) Processed lawfully, fairly and in a transparent manner and in line with the right to privacy.
- b) Collected only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with that purpose.
- c) Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is to be processed.
- d) Accurate and where necessary kept up to date.
- e) Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed.
- f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and accidental loss, destruction, or damage.
- g) Not transferred out of Kenya unless there is proof of adequate data safeguards/ measures or consent from the data subject.

7. Data protection officer

FSD Kenya has designated the **Chief Operating Officer** to be the Data Protection Officer (DPO). Accordingly, the DPO will:

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

FSD Kenya's DPO can be contacted via the email: dataprotection@fsdkenya.org.

8. Duty to notify

FSD Kenya has a duty to notify data subjects of their rights before processing data. FSD Kenya will therefore inform the data subjects of their right:

- a) To be informed of the use to which their personal data is to be put.
- b) To access their personal data in FSD Kenya's custody.
- c) To object to the processing of all or part of their personal data.
- d) To the correction of false or misleading data.
- e) To deletion of false or misleading data about them.

9. Lawful and fair processing of data

FSD Kenya will only process data where they have a lawful basis to do so. Processing personal data will only be lawful where the data subject has given their consent for one or more specific purposes or where the processing is deemed necessary:

- a) For the performance of a contract to which the data subject is a party (for instance a contract of employment).
- b) To comply with the FSD Kenya's legal obligations.
- c) To perform tasks carried out in the public interest or the exercise of official authority.
- d) To protect the vital interests of the data subject or another person.
- e) To pursue FSD Kenya's legitimate interests where those interests are not outweighed by the interests and rights of data subjects.
- f) For historical, statistical, journalistic, literature and art or scientific research.

10. Minimisation of collection

FSD Kenya will not process any personal data for a purpose for which it did not obtain consent. Should such a need arise, then consent must be obtained from the data subject.

FSD Kenya will collect and process data that is adequate, relevant, and limited to what is necessary. FSD Kenya staff must not access data which they are not authorised to access nor have a reason to access.

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.

11. Accuracy of data

FSD Kenya must ensure that the personal data it collects and processes is accurate, kept up to date, corrected or deleted without delay. All relevant records must be updated should staff be notified of inaccuracies. Inaccurate or out of date records must be deleted or destroyed.

12. Safeguards and security of data

FSD Kenya has instituted data security measures which are laid out in the Information security policy and procedures. These measures serve to safeguard personal data and must be complied with accordingly.

13. Consent

Where necessary, FSD Kenya will maintain adequate records to show that consent was obtained before personal processing data. Data will not be processed after the withdrawal of consent by a data subject.

14. Processing data relating to a child

FSD Kenya 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 FSD Kenya Safeguarding policy.

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

15. Data protection impact assessment

FSD Kenya 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 DPO to carry out the impact assessment.

16. Processing sensitive personal data

FSD Kenya will process sensitive personal data only when:

- a) 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 FSD Kenya, and the personal data is not disclosed outside that FSD Kenya without the consent of the data subject.
- b) The processing relates to personal data that has been made public by the data subject.
- c) Processing is necessary for:
 - i. The establishment, exercise or defence of a legal claim.
 - ii. The purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject.
 - iii. Protecting the vital interests of the data subject or another person where the data subject is physically or legally incapable of giving consent.

17. Transferring personal data out of Kenya

FSD Kenya will transfer personal data out of Kenya only when they have:

- a) Proof of appropriate measures for security and protection of the personal data, and the proof provided to the Data Protection Commissioner in accordance with Kenya's Data Protection Act, 2019, such measures include that data is transferred to jurisdictions with commensurate data protection laws.
- b) The transfer is necessary for the performance of a contract, implementation of pre-contractual measures such as:
 - i. For the conclusion or performance of a contract to which the data subject is part of.
 - ii. For matters of public interest.
 - iii. For legal claims.
 - iv. To protect the vital interests of data subjects.
 - v. 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.

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

18. Onward reporting

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

FSD Kenya 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.

19. Training and awareness

FSD Kenya will train staff on the contents and implementation of this policy. Staff who join FSD Kenya will be required to go through an induction process that entails familiarisation with this policy.

FSD Kenya will ensure that the requirements of this policy form part of its agreement with its grantees, contractors and third parties who process FSD Kenya's data.

20. Grantees or partners

Grantees and partners of FSD Kenya must report breaches of FSD Kenya's data in their custody within 48 hours using the emails provided above.

Grantees and partners must also abide by this policy and institute adequate mechanisms to safeguard the privacy of individuals data.

21. Roles and responsibilities

All staff must:

- a) Read, understand and comply with the contents of this policy
- b) Report suspicions of breaches promptly

All project leads and managers must

- a) Ensure staff and third parties they work with are aware of the contents of this policy
- b) Conduct risk assessments, and update controls and procedures to mitigate the risk of data breaches

The Chief Executive Officer (CEO) and Chief Operations Officer (COO) are responsible for ensuring employees, Programme Investment Committee (PIC) members, consultants, vendors, and partner organisations 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.

The PIC will provide governance oversight of activities under this policy.

The Trustees will ensure that there are adequate and effective systems and process in place to safeguard data.

22. Independent assurance

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

23. Data retention

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

24. Review of this policy

The Chief Operating Officer is responsible for ensuring that this policy is reviewed on a timely basis. This policy will be reviewed after every two years and accordingly approved by the PIC and the Trustees.

25. Related policies

This policy should be read in conjunction with:

- a) Code of conduct
- b) Misconduct, disciplinary and grievance policy
- c) Information security policy