BFA Global Kenya Ltd

Institutional Personal Data Protection Policy

July 2024

Contents

Preamble

This policy provides binding guidelines to BFA Global Kenya Ltd (BFA Global - Kenya) on how BFA Global - Kenya governs and protects personal data in compliance with the Data Protection Act, 2019, and all other applicable laws.

In addition to following the guidelines set out in this policy, BFA Global - Kenya employees, consultants, partners, and agents are bound by their respective professional standards and ethical practices as well as by all applicable international and national laws and regulations for the collection, storage, protection, and transfer of personal data. This policy is guided by the Data Protection Act, 2019, Regulations under the Act, and Guidelines issued by the Office of the Data Protection Commissioner. It aligns with international best practices in the collection, processing, storage, and transfer of data.

This policy is the basis through which BFA Global - Kenya ensures high standards of personal data governance are maintained. This policy along with other relevant BFA Global - Kenya institutional policies provides guidance on matters related to personal data protection.

This policy shall be read together with BFA Global's Data Protection Binding Corporate Rules.

In line with the above, BFA Global - Kenya's institutional personal data protection policy states as follows –

1. Guiding principles

This policy is guided by the following principles in relation to personal data protection -

a) Upholding the right to privacy of data subjects;

b) Free, prior, and informed consent for personal data collection, processing, storage, and transfer;

c) Collecting, processing, storing, and transferring personal data for expressly specified purposes;

d) Ensuring that personal data processed is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

e) Striving for accuracy of personal data;

f) Maintaining transparent and reliable records of data access, processing, storage and transfer;

g) Ensuring confidentiality and security of all data held by BFA Global - Kenya;

h) Ensuring accountability in the processing of data; and

i) Creating and developing an institutional culture of data governance and data protection.

j) Overall compliance with prevailing legal principles, rules, and international best practices when collecting, processing, storing, and transferring personal data;

2. Definitions

For purposes of this policy, the definitions in Annex 1 shall apply.

3. BFA Global - Kenya data processing

BFA Global - Kenya Data Processes data in the following main areas of work:

a) **Digital innovation:** BFA Global - Kenya designs, prototypes, and grows solutions that enable underserved individuals and businesses to better leverage the digital economy to grow their businesses and improve their livelihoods.

b) **Venture acceleration and impact investing:** BFA Global - Kenya supports startups at the forefront of inclusive tech innovation, providing bespoke venture-building support, investment readiness, and 1:1 connections with investors and corporate partners.

c) **Research and advisory:** BFA Global - Kenya's experienced researchers derive rich insights from qualitative and quantitative research, which informs BFA Global - Kenya's business, technical, financial, and policy advisory services.

d) **Learning and influence:** BFA Global - Kenya applies rigorous thinking across projects and shares lessons, insights, and proof points with the wider industry to spur further innovation for underserved communities.

4. Resources

BFA Global - Kenya shall allocate adequate resources, including personnel, finances, technology, and expertise, to ensure compliance with relevant laws and regulations pertaining to personal data protection and with this policy.

5. Data sources

The primary data sources include -

a) Personal data: this includes data relating but not limited to personal data of BFA Global - Kenya partners, BFA Global - Kenya employees, BFA Global - Kenya consultants, BFA Global - Kenya vendors, and BFA Global - Kenya agents;

b) Institutional data that does not contain personal data: this relates to BFA Global - Kenya financial data, human resources data, and other relevant operational data; and

c) Public data: this includes data available in the public domain whether online or offline.

6. Basis for collection, processing, storage, and transfer of data

BFA Global - Kenya shall collect, process, store, and transfer personal data -

a) Where free, prior, and informed consent has been obtained from the data subject;

b) Where the law requires it;

c) Where it is necessary for the performance of a contract;

d) Where it is in BFA Global – Kenya's legitimate interests to develop, build, implement, and run operational models and systems that protect its core mandate and provide its partners with a high standard of service;

e) BFA Global – Kenya's interests to prevent and investigate statutory, regulatory, or policy violations;

f) To verify BFA Global - Kenya employee's/consultant's/vendor's/agent's identity to protect its core mandate to comply with laws that apply to it; or

g) Where it is in BFA Global – Kenya's legitimate interests to provide information about its operations and services that it considers would benefit or inform its employees, consultants, vendors, and/or agents.

7. Professional ethical standards

In addition to this policy, all BFA Global – Kenya professionals shall abide by their respective professional ethical standards related to personal data governance and protection. Such professionals may include lawyers, auditors, medical professionals, research professionals, and accountants working at BFA Global - Kenya.

8. Personal data

Where BFA Global - Kenya collects, processes, stores, and transfers personal data, the following principles shall apply –

a) Free, prior, and informed consent given by the data subject for BFA Global - Kenya to collect, process, store, and transfer their data;

b) Data collected, processed, stored, and transferred in a lawful, fair, and transparent manner;

c) Data collected, processed, stored, and transferred for a specified and legitimate purpose;

d) Only relevant personal data is processed;

e) Ensure the accuracy of the data and the right of the data subject to correct any faulty data relating to them;

f) Ensure the security of personal data held by BFA Global - Kenya;

g) Right of the data subject to object to the collection, processing, storage, or transfer of their data;

h) Right of the data subject to be provided with copies of data about them that is held by BFA Global - Kenya; and

i) Data is processed, stored, and transferred in a manner that does not unnecessarily identify or expose the data subject to risk.

9. Data subject rights

BFA Global - Kenya shall respect the rights of data subjects including but not limited to the following:

a) **Right to access**: Data subjects have a right to obtain confirmation from BFA Global - Kenya as to whether personal data concerning them is being processed, and, where that is the case, access to such personal data and related information.

b) **Right to rectification:** Data subjects have a right to request the rectification of inaccurate or incomplete personal data concerning them held by BFA Global - Kenya.

c) **Right to erasure:** Data subjects have a right to request the erasure of personal data concerning them, where the data is no longer necessary for the purposes for which it was collected, or where they withdraw their consent.

d) **Right to restriction of processing:** Data subjects have a right to request the restriction of processing of their personal data in certain circumstances, such as when the accuracy of the data is contested, or the processing is unlawful.

e) **Right to data portability:** Data subjects have a right to receive the personal data concerning them, which they have provided to BFA Global - Kenya, in a structured, commonly used, and machine-readable format, and to transmit that data to another controller without hindrance.

f) **Right to object:** Data subjects have a right to object to the processing of their personal data, including processing for direct marketing purposes or where the processing is based on legitimate interests pursued by BFA Global - Kenya.

g) **Rights in relation to automated decision-making and profiling:** Data subjects have a right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

10. Data subject requests

a) The BFA Global Data Protection Officer will handle data subject requests in consultation with the BFA Global - Kenya Data Protection Committee.

b) The Data Protection Officer, in consultation with the BFA Global - Kenya Data Protection Committee, shall address data subject requests, paying attention to, among other things, the data subjects' rights and BFA Global - Kenya's legal exposure.

c) Data subject requests shall be in line with the Data Protection Act and PART II of the Data Protection (General) Regulations.

d) Response to data subject requests shall comply with the timelines set out under the Data Protection Act and PART II of the Data Protection (General) Regulations.

e) BFA Global - Kenya employees shall support the Data Protection Officer and Data Protection Committee when they address data subject requests.

Data subject requests shall be recorded as follows:

Date of Request	Data Subject Details	Nature of Request	Action Taken	Date Data Subject is Informed of Action Taken

11. Collection of data

Data shall as much as possible be collected from the source –

a) Personal data shall as far as is practicable be collected directly from the data subject unless the data is public record, has been made public by the data subject, has been provided by a legal guardian or the data subject has consented to BFA Global - Kenya collecting the data indirectly.

b) Institutional data shall be collected directly from the relevant BFA Global - Kenya administrative units.

Collection of data shall only be undertaken in line with this policy.

12. Privacy notice

Where applicable, any person collecting personal data for or on behalf of BFA Global - Kenya shall provide and explain to the data subject the provisions of BFA Global – Kenya's privacy notice. The privacy notice shall set out:

a) Types of data being processed by BFA Global - Kenya.

b) Purpose of data processing.

c) Legal basis for data processing.

d) Any third parties BFA Global - Kenya shares the processed data with.

e) Data retention periods.

f) How BFA Global - Kenya will keep the data secure.

g) Data subject rights and how data subjects may exercise those rights at BFA Global - Kenya.

h) BFA Global - Kenya Data Protection Officer's contact information.

i) Office of the Data Protection Commissioner's contact information

The privacy notice shall be made available on BFA Global - Kenya's website, availed to data subjects at the point of data collection, or explained to the data subject orally.

13. Data processing

Processing of data shall be in line with the purpose of collection.

14. Data storage

a) Data shall be stored in forms and media, including digital or otherwise, as approved by BFA Global—Kenya's Management Team.

b) No person shall store data other than in the approved formats under this policy.

15. Data retention

a) Personal data shall be retained for the period necessary for the purpose for which the data was processed.

b) Institutional data shall be retained for a period minimum period of seven (7) years.

Data will be destroyed periodically in line with BFA Global's administrative guidelines and relevant statutory provisions.

BFA Global - Kenya shall keep a data retention record in the following manner:

BFA Global - Kenya data retention schedule				
Data Type	**Storage location**	**Retention period**	**Reason for retention**	**Action (delete or archive)**

16. Data accuracy

a) BFA Global - Kenya staff/consultants/vendors engaged in personal data collection and processing shall take measures to verify whether the data obtained is accurate and up to date.

b) In case of inaccuracies or inconsistencies in the data, they shall inform the data subjects or any other data sources and either request corrected data or obtain authorization to correct the errors identified.

17. Data security and breach response

a) Only authorized persons shall have access to personal data.

b) Appropriate measures shall be undertaken to ensure that no unauthorized persons access, alter, or destroy data.

c) Electronic data security shall be in line with the prevailing Information, Committee and Technology (ICT) and Cyber Security policy.

d) If a confirmed data breach involving personal data occurs, BFA Global—Kenya's Management Team will be notified within twenty-four (24) hours.

e) In case of a confirmed data breach relating to institutional data, BFA Global – Kenya's Management Team shall be notified within twenty-four (24) hours.

f) Notification of a data breach to the Office of the Data Commissioner shall be done within 72 hours in accordance with the Data Protection Act and Part IV of the Data Protection (General) Regulations.

For any incident or breach, the record in Annex 2 shall be kept and provided to the Office of the Data Commissioner.

BFA Global - Kenya incident/breach response plan shall be as detailed in Annex 3.

18. Data from external sources

Where BFA Global—Kenya receives/obtains personal data from external sources, assurance shall be sought and provided to confirm whether the data was received/obtained in accordance with relevant data protection laws.

19. Data transfer

No data shall be transferred to a third party without authorization from the Chief Executive Officer following the advice of the Data Protection Officer or in the case of personal data without the express consent of the data subject.

Data shall only be transferred to persons and institutions that have undertaken sufficient measures to ensure data privacy and protection.

20. Vendor risk assessment

Before engaging a vendor to process personal data for or on behalf of BFA Global—Kenya, a risk assessment shall be carried out using the template in Annex 4.

Where the consultant/ vendor is an individual, BFA Global - Kenya shall have them sign a commitment to ensuring compliance with the Data Protection Act, Regulations, and this Policy.

21. Anonymization and pseudonymization

Where pseudonymization or anonymization techniques are used to protect personal data against unwanted disclosure or use, their effectiveness shall be monitored, considering advances in techniques for re-identifying supposedly anonymized or pseudonymized data.

22. Encryption

Digital records shall be processed behind strong authentication, and authorization measures and have strong forms of protection including encryption of files in line with the prevailing ICT and Cyber Security policies.

23. Handling sensitive data

a) Sensitive data shall be labeled with a risk level that determines the handling methods and resources, the required encryption level, and the storage and transmittal requirements.

b) Data shall be categorized as -

i. Public for general data accessible by the general public, partners, employees, agents, consultants, and service providers;

ii. Internal use for data accessible to employees only; and

iii. Confidential data is accessible only to authorized individuals.

24. Data Inventories

All functions/departments/units at BFA Global - Kenya shall keep updated data inventories. The Data Protection Officer and the Data Protection Committee shall regularly review BFA Global – Kenya's data inventory. The inventory shall be in the format in Annex 5.

25. Complaints

a) BFA Global - Kenya has an internal personal data complaints mechanism.

b) Complaints relating to personal data shall first be handled by the Data Protection Officer in consultation with BFA Global—Kenya Data Protection Committee.

c) The Data Protection Officer, in consultation with the Data Protection Committee, shall ensure that all complaints are handled in-house through alternative dispute resolution mechanisms.

d) BFA Global—Kenya employees shall support the Data Protection Officer and Data Protection Committee when they address personal data complaints.

26. Data Protection Officer

a) BFA Global—Kenya's Management Team shall designate at least one team member to collaborate with BFA Global's Data Protection Officer.

b) As required under Section 24(7) of the Data Protection Act, the BFA Global Data Protection Officer shall -

- advise BFA Global - Kenya on data processing requirements provided under the Data Protection Act or any other written law;
- ensure on behalf of BFA Global - Kenya that the Act is complied with;
- facilitate capacity building of staff and partners involved in data processing operations;
- carry out continuous data protection audits of BFA Global - Kenya operations;
- provide advice on data protection impact assessments;
- coordinate data access requests made to BFA Global - Kenya;
- coordinate BFA Global – Kenya's data protection-related complaints processes;
- review documents/agreements/terms and conditions/policies/contracts to ensure they are aligned to provisions of the Data Protection Act;
- coordinate data breach preparedness and response with BFA-GLOBAL KENYA;

- co-operate with the Data Commissioner and any other authority on matters relating to data protection;
- be the chairperson of BFA Global – Kenya's Data Protection Committee; and
- submit quarterly data protection compliance reports BFA Global – Kenya's Management Team.

c) When in doubt about the processing of personal data at BFA Global - Kenya, an employee/agent/partner/consultant of BFA Global - Kenya shall consult the Data Protection Officer for guidance.

d) All BFA Global - Kenya, employees, agents, partners, and consultants shall provide the Data Protection Officer with all the necessary information, support, and guidance.

27. BFA Global - Kenya Data Protection Committee

Members:

a) Chairperson – Data Protection Officer

b) Member - CEO

c) Member – Legal Representative

d) Member - Human Resource Representative

e) Member – Finance Representative

f) Member – ICT Representative

BFA Global – Kenya's Data Protection Committee shall -

a) Meet semi-annually to review the progress of data protection management within BFA Global - Kenya to support the Data Protection Officer;

b) Meet on an *ad hoc* basis in the case of arising critical data protection issues;

c) Promote a culture of good data governance within BFA Global - Kenya;

d) Act as data protection champions within their departments/functions; and

e) Provide advice to the Data Protection Officer on data governance matters.

28. Communication on data matters

a) Information arising or relating to any issue under this policy shall be communicated by the Data Protection Officer.

b) Any communication containing data shall have a cautionary notice stating that the recipients shall uphold BFA Global - Kenya's data protection policy.

29. Non-disclosure agreements

All employees, agents, consultants, and vendors who process personal data shall sign a non-disclosure agreement before being formally engaged in any contractual obligations. This policy shall form part of the non-disclosure agreement.

30. Data protection compliance assessments

a) The Data Protection Officer shall undertake data protection compliance assessments semi-annually and submit an annual report to BFA Global – Kenya's Management Team.

b) The data protection compliance assessment shall:

   i. describe the nature, scope, context, and purposes of the assessment;

   ii. assess necessity, proportionality, and compliance measures to this policy;

   iii. identify and assess risks to privacy and data protection; and

   iv. identify measures to mitigate those risks.

31. Cooperation with regulators

a) Cooperation with the Office of the Data Protection Commissioner is paramount. BFA Global – Kenya shall provide a Regulator with all the necessary information required as per the Data Protection Act.

b) BFA Global – Kenya shall respect and abide by the advice/direction of a Regulator on any issues regarding data protection compliance.

32. Non-compliance

Non-compliance with this policy for partners, employees, agents, consultants, and suppliers, the matter shall be dealt with in accordance with the contractual obligations in force.

33. Review and revision

This policy shall be subject to regular review and, where necessary, revision to reflect changes in legal or regulatory requirements, organizational practices, or technological advancements.

34. Effective date

This policy shall come into force on **1 August 2024**.

Annexures

Annex 1. Definitions

"agent" means a person authorized to act for BFA Global - Kenya through a contract of employment, or any other contract, or apparent authority;

"consultant" means a person under contract or otherwise providing professional advice to BFA Global - Kenya;

"data" in general includes information in raw, organized, or unorganized form that refers to, or represent, conditions, ideas, facts, statistics, or objects.

"data subject" means a natural person that is the subject of personal data processing;

"employee" means a person employed for wages or a salary and includes an apprentice and indentured learner;

"personal data" means any information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly in particular by reference to an identification criterion or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity;

"Processing" means any operation or set of operations which is performed upon data, whether or not by automatic means such as collection, recording, organization, storage, adaptation, alteration, retrieval, backup, copy, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination and locking, encryption, erasure or destruction of data;

"sensitive data" may include data identified as such by Data Protection Officers or personal data that consists of racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation;

"Third-party" means any public or private individual or legal entity, body, or association other than the data subject or BFA Global - Kenya or any person who is authorized to collect, process, or transfer data in line with this policy;

"vendor" refers to a third-party company or service provider that processes personal data on behalf of BFA Global - Kenya.

Annex 2. Incident and data breach register

Incident and data breach register	
Breach ID	
When BFA Global - Kenya became aware of the breach	
Date breach occurred	
Time breach occurred	
Classes of data compromised	
How breach occurred	

Nature of breach	
Cause of breach	
Who is responsible for the breach	
Data subjects affected	
Risk and potential harm to data subjects	
Action to be taken by data subjects to reduce harm	
Effect of the breach to BFA Global – Kenya operations	
Remediation measures undertaken by the BFA Global – Kenya	
Notification to data subjects	
Notification to ODPC	
Remediation measures – long term	
Lessons learned	
Contact of BFA Global - Kenya DPO	

Annex 3. Data breach/ incident response plan

Preparation	
Cybersecurity policy in place	
Data protection policy in place	
Staff have received incident response training	
There is an incident log report template	
Arrangements for service providers, including cloud and software as a service, to provide and retain logs have been established and tested to ensure these include useful data and can be provided in a timely manner.	
BFA Global - Kenya has internal or third-party arrangements and capabilities to detect and analyse incidents	
Critical assets (data, applications, and systems) have been identified and documented	
Detection, investigation, analysis and activation	
Detection mechanisms, such as scanning, senses, and logging mechanisms, can be used to identify potential information security incidents. These mechanisms require monitoring processes to identify unusual or suspicious activity, such as behavior and logging, commensurate with the impact of an incident.	

Incident detection, including self-detected incidents, notifications received from service providers or vendors, and notifications received from trusted third parties.	
Incident analysis, including how incidents are to be categorized, classified, and prioritized, and controls related to how data is stored and transmitted.	
Activating an Incident Response Team to manage critical incidents, with roles and responsibilities assigned.	
Activating a Senior Management Team to manage critical incidents, with roles and responsibilities assigned.	
Containment, evidence collection, and remediation	
Roles and responsibilities assigned for containment, evidence collection, and remediation.	
Communications	
Templates have been developed to support communicating with: • Internal stakeholders • External stakeholders	
Incident notification and reporting	
Processes and contact details are documented to support BFA Global—Kenya in meeting its legal and regulatory requirements on incident notification, reporting, and response. Roles and responsibilities within BFA Global—Kenya are assigned. This includes the processes for obtaining authority to release and share information.	
Post-incident review	
A process is documented for conducting Post-Incident Reviews (PIR) following the conclusion of an incident. PIR reports with recommendations are submitted to management for endorsement.	
A process is documented to ensure actions following incidents and/or exercises are tracked and completed.	

Annex 4. Vendor risk assessment

Question	Responses
1. Why does BFA Global - Kenya require the services of the vendor?	
2. For how long will the vendor be contracted?	
3. Has BFA Global - Kenya contracted the vendor before?	
4. What is the legal status of the vendor?	

5. What personal data will the vendor process?	
6. Does the vendor have an in-house data protection policy in place?	
7. Does the vendor have a designated Data Protection Officer?	
8. Does the vendor have a privacy notice in place?	
9. How many employees of the vendor are aware of their obligations under the Data Protection Act?	
10. Does the vendor have an in-house data protection complaint handling mechanism?	
11. How will the vendor process personal data on behalf of BFA Global - Kenya?	
12. What measures has the vendor put in place to ensure the security of the personal data it processes?	
13. Will the vendor subcontract its services?	
14. Will the vendor carry out international transfers of data?	
15. How many breaches has the vendor experienced in the last three years?	
16. Does the vendor have pending complaints or lawsuits relating to personal data protection?	
17. Is the vendor registered with the Office of the Data Protection Commissioner?	
18. Is there a contract between BFA Global - Kenya and the vendor?	
19. Will the vendor be a processor or joint controller?	

Annex 5. Data inventory details

Department:	
Applicable Law	
Data subjects	
Data elements collected	
Sensitive data elements	
Mode of collection	
Legitimate use	
Departments handling the data	
Technology in use	

Location	
Risks	
Risk mitigation	
Third parties processing the data	
Retention period	