Bankable Frontier Associates LLC
(BFA Global)

Data Protection Policy
(Binding Corporate Rules)

July 2024

Contents

1. Introduction....3
2. Scope....3
3. Guiding principles....3
4. Definitions....4
5. BFA Global data processing....4
6. Resources....4
7. Governance structure....4
8. Data sources....5
9. Privacy by design....5
10. Data security by design....5
11. Basis for collection, processing, storage, and transfer of data....5
12. Data subject rights....5
13. Exercise of data subject rights....6
14. Purpose limitation....7
15. Data minimization....7
16. Data quality....7
17. Data storage....7
18. Data retention....7
19. Data security....7
20. Data breach response....8
21. Data from external sources....8
22. Transparency....8
23. Data transfers....8
24. Training and awareness:....9
25. Vendor risk assessment....9
26. Audit....9
27. Documentation and record-keeping....9
28. Cooperation with regulators....10
29. Non-compliance....10
30. National laws and binding corporate rules....10
31. Review and revision....10
32. Effective date....10
Annexures:....11
    Annex 1. Definitions....11
    Annex 2. Vendor risk assessment questionnaire....12

1. Introduction

BFA Global is an impact innovation firm that combines research, advisory, venture building, and investment expertise to build a more inclusive, equitable, and resilient future for underserved people and the planet. BFA Global partners with leading public, private, and philanthropic organizations, global and local, to catalyze innovation ecosystems for impact across emerging markets.

Founded in 2006, BFA Global is headquartered in Nairobi and Boston, with a presence in Medellín, New Delhi, Mexico City, Lagos, Madrid, London, and Paris.

BFA Global is committed to ensuring an adequate level of personal data protection at all BFA Global offices. Social, cultural, and regulatory differences between the country offices shall not affect the adequate level of personal data protection. BFA Global employees, clients, vendors, and partners can rely on the promise that BFA Global will treat personal data in all offices in an equally secure and responsible way.

The objective of these Binding Corporate Rules (Rules) is to provide adequate protection for the transfers and processing of personal data by BFA Global offices. BFA Global can only achieve this goal of providing an adequate level of data protection if all BFA Global offices and every single employee, consultant, agent, and vendor accept the Rules as binding. It is the duty of all BFA Global offices, consultants, vendors, agents, and employees to always abide by the Rules.

BFA Global acknowledges that maintaining an adequate level of personal data protection demands continuous efforts of all BFA Global stakeholders. BFA Global will ensure compliance with the Rules. The audit scheme, which is part of the Rules helps BFA Global to monitor the personal data protection processes.

2. Scope

These Rules are the framework for data protection compliance within BFA Global. They facilitate the lawful collection, storage, transfer, and destruction of personal data while at rest and when in motion, including across borders. These Rules provide the mechanism for BFA Global to transfer personal data across borders within the organization. They are designed to ensure a high level of protection for data subjects' rights and freedoms.

3. Guiding principles

These Rules are guided by the following principles in relation to personal data governance and protection:

a) Free, prior, and informed consent for personal data collection, processing, storage, and transfer.

b) Compliance with prevailing legal principles, rules, and international best practices when collecting, processing, storing, and transferring personal data.

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 the 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.

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

4. Definitions

For purposes of these Rules, the definitions in Annex 1 shall apply.

5. BFA Global data processing

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

a) **Digital innovation:** BFA Global 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 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's experienced researchers derive rich insights from qualitative and quantitative research, which informs BFA Global's business, technical, financial, and policy advisory services.

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

6. Resources

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

7. Governance structure

BFA Global shall appoint a Data Protection Officer to oversee and ensure compliance with these Rules. The Data Protection Officer shall:

a) advise country offices and the management team on compliance with these Rules and country-specific regulatory requirements,

b) deal with Data Protection Authorities and Regulators' investigations and requests,

c) ensure resources are allocated toward personal data protection compliance,

d) conduct personal data protection assessments and audits,

e) provide leadership in handling data subject requests,

f) provide leadership in the incident and data breach response strategies,

g) ensure impeccable record keeping related to personal data protection compliance, and

h) provide reports on data protection compliance status.

8. Data sources

The primary data sources for BFA Global include:

a) Personal data: This includes, but is not limited to, personal data from BFA Global partners, employees, research subjects, consultants, clients, vendors, and agents.

b) Institutional data: this relates to BFA Global financial data, human resources data, and other relevant operational data.

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

9. Privacy by design

BFA Global shall adopt a proactive approach to privacy by considering privacy implications from the outset of any new project, product, or service.

Privacy-enhancing measures shall be built into systems and processes by default, with privacy being the default setting.

10. Data security by design

Security measures shall be tailored to address the specific risks and threats associated with the processing of personal data by BFA Global, based on comprehensive risk assessments.

Security measures shall include encryption, anonymization and pseudonymization of data, identity and access management, data integrity, and incident response strategies.

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

BFA Global shall collect, process, store, and transfer personal data:

a) Where free prior and informed consent is required 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's legitimate interests to develop, build, implement, and run strategies and systems that protect its core mandate and provide its partners with a high standard of service.

e) BFA Global's interest is to prevent and investigate corporate and statutory violations.

f) To verify the partner's/employee's/consultant's/vendor's/agent's identity to protect its core mandate to comply with laws that apply to it.

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

12. Data subject rights

BFA Global 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 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.

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, 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.

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.

13. Exercise of data subject rights

a) Data subjects may exercise their rights by submitting a written request to BFA Global.

b) BFA Global shall respond to data subject requests without undue delay and within stipulated respective country-specific statutory timelines.

c) BFA Global Data Protection Officer shall handle data subject requests and complaints.

d) Data subject requests shall be handled by the Data Protection Officer in consultation with the BFA Global Data Protection Committee.

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

f) BFA Global employees shall support the Data Protection Officer and Data Protection Committee when they are addressing 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

BFA Global contacts to be provided to data subjects is privacy@bfaglobal.com.

14. Purpose limitation

Personal data should only be processed and transferred if it is necessary for the specific and legitimate purposes of BFA Global's work, operations, and mandate.

If personal data is processed for purposes other than the original ones, direction and counsel should be sought from the relevant country's Legal Counsel and Data Protection Officer.

15. Data minimization

BFA Global shall collect personal data directly from data subjects wherever possible and shall refrain from collecting unnecessary or excessive data. Unless it runs contrary to the intended work, operations, or mandate, BFA Global will prefer to collect anonymized or pseudonymized data.

16. Data quality

The offices and employees of BFA Global shall take reasonable steps to ensure that the personal data processed is accurate, complete, and current.

BFA Global requires that employees, research subjects, consultants, agents, vendors, and partners provide accurate, complete, and current data for processing.

Personal data processed at BFA Global that is inaccurate, incomplete, or not current shall be corrected, completed, or updated as necessary. Where an update of data is not possible the data may be deleted or archived.

17. Data storage

Data shall be stored in forms and media which may be digital or otherwise as approved by BFA Global's management in consultation with BFA Global's staff.

No person shall store data other than in the approved formats under these rules.

18. Data retention

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

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

19. Data security

BFA Global offices, employees, consultants, agents, vendors, and stakeholders shall take reasonable precautions to protect personal data from loss, misuse, and unauthorized access, disclosure, alteration, and destruction.

BFA Global shall have technical and organizational measures which comprise physical access control, system access control, logical access control, disclosure control, input control, job control, availability control, and separation control.

Data security shall also comply with the prevailing BFA Global ICT policy and other standard operating procedures and guidelines.

20. Data breach response

In case of a confirmed personal data breach, all BFA Global offices shall be notified immediately after the breach is confirmed.

The Data Protection Officer shall designate a team to address the data breach. The team shall be comprised of the Data Protection Officer, CEO, ICT Officer, Chief Finance Officer, Human Resources Officer, Legal Officer, and Risk and Compliance Officer.

The data breach response team shall set out measures upon discovering the data breach, including containment, risk assessment, mitigation measures, and communication protocols.

The respective Data Protection Officer shall notify the relevant Regulator(s)/Data Protection Authority within stipulated statutory timelines.

21. Data from external sources

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

22. Transparency

BFA Global shall make these Rules readily available to every data subject to maintain transparency about the way BFA Global treats personal data and informs them about their rights.

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

a) Types of data being processed by BFA Global.

b) Purpose of data processing.

c) Legal basis for data processing.

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

e) Data retention periods.

f) How BFA Global will keep the data secure.

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

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

23. Data transfers

BFA Global country offices only disclose personal data to processors if it is necessary to achieve a specific purpose.

Data shall only be transferred to parties that have appropriate safeguards.

BFA Global country offices shall conclude a written agreement with external data processors that they can only act under instructions from BFA Global and are responsible for appropriate measures to ensure the security and confidentiality of data processing.

All transfers of data to external controllers or processors shall respect local transborder data flow regulations.

24. Training and awareness:

BFA Global will carry out frequent and special training to ensure that all the employees have a sound understanding of the requirements of these Rules and all relevant data protection regulations.

The Data Protection Officer will monitor the execution of the training.

25. Vendor risk assessment

Vendor risk assessment shall be carried out before engaging a vendor who shall process personal data for or on behalf of BFA Global, where:

a) the vendor is expected to supply goods/ services worth more than USD 10,000 in a year; or

b) where the vendor is expected to handle sensitive data regardless of the value of the goods/ services

The template in Annex 2 will be used.

Where the consultant/ vendor is an individual, BFA Global shall have them sign a commitment to ensure compliance with these Rules and local privacy and data protection laws.

26. Audit

To ensure compliance with these Rules, BFA Global management will initiate and oversee audits on a regular basis.

Data protection compliance audits shall be undertaken both internally and externally. Internally by the respective internal auditors in collaboration with the Data Protection Officer. Externally by a duly appointed data protection audit specialist.

The audits shall cover all aspects of these Rules, including methods of ensuring that corrective actions and measures are implemented to achieve compliance.

Audit reports shall be considered by BFA Global management.

27. Documentation and record-keeping

BFA Global shall maintain accurate and up-to-date records of its data processing activities, including but not limited to:

a) The types of personal data processed.

b) Purposes of processing.

c) Categories of data subjects.

d) Data storage locations.

e) Data transfers, including details of recipients or third parties involved.

f) Data retention periods.

g) Security measures implemented.

h) Data protection impact assessments (DPIAs), where applicable.

i) Vendors/agents/consultants processing data.

j) Records of data subject requests and responses.

k) Data breach incidents and response actions taken.

l) Country-specific compliance records such as registration with a Regulator/Data Protection Authority.

28. Cooperation with regulators

BFA Global country offices shall cooperate and assist each other in handling an individual's request or complaint or an investigation or inquiry by Regulators/Data Protection Authorities.

Cooperation with a Regulator/Data Protection Authority is paramount. All BFA Global shall provide a Regulator/Data Protection Authority with all the necessary information required as per prevailing law and procedures. BFA Global shall respect and abide by the advice of a Regulator/Data Protection Authority on any issues regarding data protection compliance.

29. Non-compliance

Non-compliance with these Rules shall be dealt with as follows: for partners, employees, agents, consultants, and suppliers, the matter shall be dealt with in accordance with the contractual obligations in force.

30. National laws and binding corporate rules

Where the BFA Global Office local legislation, requires a higher level of protection for personal data, that law will take precedence over these Rules.

31. Review and revision

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

32. Effective date

These Rules shall come into force on 1 August 2024.

Annexures:

Annex 1. Definitions

Agent: means a person authorized to act for BFA Global through a contract of employment, or any other contract, or apparent authority;

Data: in general includes information in a raw, organized, or unorganized form that refers to, or represents, conditions, ideas, facts, statistics, or objects.

Consultant: means a person under contract or otherwise providing professional advice to BFA Global;

Consent: Freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of their personal data.

Data Breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

Data Controller: The entity that determines the purposes, conditions, and means of the processing of personal data. This could be a company, organization, or person.

Data Subject: An identifiable natural person to whom the personal data relates. This could be customers, employees, website visitors, vendors, consultants, agents, research subjects, or any individual whose data is being processed.

Data Processor: An entity that processes personal data on behalf of the data controller. This could include banks, insurance companies, cloud service providers, IT support companies, or other third-party service providers.

Data Protection Officer (DPO): A person or entity designated by the data controller or data processor to monitor compliance with these Rules and local data protection regulations, provide advice regarding data protection obligations and act as a contact point for data subjects and regulators or supervisory authorities.

Personal Data: Any information relating to an identified or identifiable natural person. This includes identifiers such as name, identification number, location data, online identifier, or factors specific to the physical, physiological, genetic, mental, economic, cultural, contact information, or social identity of that person.

Processing: Any operation or set of operations performed on personal data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

Sensitive/Special Personal Data: The definition of sensitive/special personal data may vary from country to country. BFA Global Offices shall adopt the definition set out in their local privacy and data protection laws. However, such personal data may include data related to racial or social origin, political opinions, religious and philosophical beliefs, genetic data, biometric data, gender, sex life or sexual orientation, and trade union membership.

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

Annex 2. Vendor risk assessment questionnaire

Question	Responses
1. Why does BFA Global require the services of the vendor?	
2. For how long the vendor will be contracted?	
3. Has BFA Global 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. Are the vendor's employees aware of their obligations under local privacy and data protection laws?	
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?	
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 relevant regulatory authorities?	
18. Is there a contract between BFA Global and the vendor?	
19. Will the vendor be a processor or joint controller?	