

Master Privacy Policy Template

VERSION 1.0 · CLASSIFICATION: PUBLIC

MUCHANGI PATRICK & ASSOCIATES ADVOCATES

Data Privacy · AI Governance · Digital Regulation

DOCUMENT CONTROL

ITEM	DETAILS
Template Number	MPA-DP-001
Document Type	Privacy Policy
Version	1.0
Approved By	<i>[Board / Management]</i>
Effective Date	<i>[Insert Effective Date]</i>
Next Review Date	<i>[Insert Review Date]</i>
Policy Owner	Data Protection Officer
Document Classification	Public

CONTENTS

1. Introduction
2. Scope
3. Definitions
4. Who We Are
5. Information We Collect
6. Sources of Personal Data
7. Purposes of Processing
8. Lawful Bases for Processing
9. Cookies and Similar Technologies
10. AI-Assisted Processing
11. Automated Decision-Making
12. Data Sharing
13. International Transfers
14. Data Security
15. Data Retention
16. Your Rights
17. Exercising Your Rights
18. Children's Data
19. Marketing Communications
20. Third-Party Websites
21. Changes to this Policy
22. Contact Information
23. Complaints

1. INTRODUCTION

This Privacy Policy ("Policy") explains how [Organisation Name] ("we", "us", "our", the "Organisation") collects, uses, stores, discloses, transfers and otherwise processes personal data in the course of our operations.

We are committed to safeguarding the privacy of individuals and processing personal data in accordance with Article 31 of the Constitution of Kenya, the Data Protection Act, 2019 ("the Act"), the Data Protection (General) Regulations, 2021, the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021, the Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021, and any other applicable law.

This Policy should be read alongside any specific notice provided to you at the point personal data is collected.

2. SCOPE

This Policy applies to personal data processed by [Organisation Name], whether collected directly, indirectly, digitally or in hard copy, within or outside Kenya, in relation to:

- Customers and clients
- Employees, directors and officers
- Job applicants
- Suppliers and contractors
- Website and mobile application users
- Business partners
- Service providers

3. DEFINITIONS

For the purposes of this Policy, the following terms shall bear the meanings set out below, consistent with the Data Protection Act, 2019:

- "Personal Data" means any information relating to an identified or identifiable natural person.
- "Sensitive Personal Data" means data revealing the data subject's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details, or sex or sexual orientation.
- "Processing" means any operation performed on personal data, whether or not by automated means, including collection, recording, organisation, storage, adaptation, retrieval, use, disclosure, dissemination, restriction, erasure or destruction.
- "Data Subject" means an identified or identifiable natural person who is the subject of personal data.
- "Data Controller" means a person who, alone or jointly with others, determines the purpose and means of processing personal data.

- “Data Processor” means a person who processes personal data on behalf of a data controller.
- “Consent” means an express, unequivocal, free, specific and informed indication of a data subject's wishes, signified by a statement or clear affirmative action.
- “Profiling” means automated processing of personal data used to evaluate certain personal aspects relating to a natural person.
- “Automated Decision-Making” means a decision made by automated means without human involvement, which produces legal or similarly significant effects on a data subject.
- “Artificial Intelligence System” means a system that uses machine-based processing, including machine learning, to generate outputs such as predictions, recommendations or decisions.
- “Cookies” means small data files placed on a device when a user accesses a website.
- “Cross-Border Transfer” means the transfer of personal data to a recipient located outside Kenya.

4. WHO WE ARE

[Organisation Name] is [insert legal status, e.g. a company incorporated under the laws of Kenya], with registration number [Company Registration Number].

Registered / Principal Address: *[Insert Address]*

Email: *[Insert Email]*

Telephone: *[Insert Telephone]*

Website: *[Insert Website]*

For the purposes of the Data Protection Act, 2019, [Organisation Name] is the data controller [and, where applicable, data processor] in respect of the personal data described in this Policy.

Data Protection Officer: *[Insert DPO Name]*

DPO Email: *[Insert DPO Email]*

DPO Telephone: *[Insert DPO Telephone]*

5. INFORMATION WE COLLECT

We may collect, use, store and otherwise process the following categories of personal data about you:

Identity Data

- Name
- National ID or passport number
- Date of birth
- Gender
- Nationality
- Photograph

- Signature

Contact Data

- Email address
- Telephone number
- Postal address
- Physical address

Financial Data

- Bank account details
- M-PESA details
- Payment history
- Invoices

Technical Data

- IP address
- Browser type and version
- Operating system
- Device information
- Session data
- Log files
- Cookies

Employment Data

- Curriculum vitae
- Qualifications
- Payroll information
- Performance records
- Disciplinary records

Special Categories of Personal Data

We only collect and process the following categories of sensitive personal data where permitted by law, and subject to appropriate safeguards:

- Health data
- Biometric data
- Religion
- Ethnicity
- Political opinion
- Trade union membership
- Criminal convictions

6. SOURCES OF PERSONAL DATA

We collect personal data from the following sources:

- Directly from you
- Our website and mobile applications
- Applications and forms
- Email and telephone correspondence
- Cookies and similar technologies
- Public registers
- Government agencies
- Employers
- Service providers and business partners
- Social media platforms

7. PURPOSES OF PROCESSING

We process personal data for the purposes set out below, each of which is anchored in a lawful basis under the Data Protection Act, 2019:

PURPOSE	LAWFUL BASIS
Account creation and management	Contract
Customer support	Legitimate Interests
Legal and regulatory compliance	Legal Obligation
Recruitment	Legitimate Interests / Contract
Employment administration	Contract
Marketing communications	Consent
Security monitoring	Legitimate Interests
Fraud prevention	Legitimate Interests
Litigation and dispute resolution	Legal Obligation
Regulatory reporting	Legal Obligation
AI-assisted customer support	Legitimate Interests (subject to safeguards)

8. LAWFUL BASES FOR PROCESSING

We rely on one or more of the following lawful bases recognised under the Data Protection Act, 2019 to process personal data:

- Consent — where you have given clear, informed consent to the processing.
- Contractual necessity — where processing is necessary for the performance of a contract with you, or to take steps at your request prior to entering a contract.
- Compliance with a legal obligation — where processing is necessary for us to comply with the law.

- Protection of vital interests — where processing is necessary to protect your life or the life of another person.
- Legitimate interests — where processing is necessary for our legitimate interests, or those of a third party, provided such interests are not overridden by your interests, rights or freedoms.
- Public interest or exercise of official authority — where applicable to the Organisation's functions.

9. COOKIES AND SIMILAR TECHNOLOGIES

Our website uses cookies and similar tracking technologies to distinguish you from other users, improve functionality and analyse website usage. We use the following categories of cookies:

- Essential cookies, necessary for the website to function
- Analytics cookies, used to understand website usage
- Marketing cookies, used to deliver relevant advertising
- Preference cookies, used to remember your settings and choices

You may manage or withdraw your consent to non-essential cookies at any time through your browser settings or our cookie preference tool. Further detail is set out in our separate Cookie Notice.

10. AI-ASSISTED PROCESSING

The Organisation may use Artificial Intelligence systems to assist with activities such as document analysis, customer support, fraud detection, cybersecurity monitoring and operational efficiency.

Where AI systems are used to process personal data:

- AI outputs are subject to human oversight where appropriate.
- AI systems are not used as the sole basis for decisions that produce legal or similarly significant effects on individuals, unless authorised by law and accompanied by appropriate safeguards.
- AI processing is carried out in accordance with applicable data protection obligations and the Organisation's internal AI governance measures.

11. AUTOMATED DECISION-MAKING

[State whether the Organisation uses automated decision-making, including profiling. Where used, describe the logic involved, the significance and the envisaged consequences of such processing.]

- Whether automated decision-making is used, and for what purpose
- How the automated process works, in broad terms
- Your right to request human intervention in the decision
- Your right to express your point of view and to contest the decision

12. DATA SHARING

We may share personal data with the following categories of recipients, where necessary for the purposes described in this Policy and subject to appropriate contractual and technical safeguards:

- Banks and payment providers
- Cloud and IT service providers
- Law firms and professional advisers
- Auditors
- Regulators and government agencies
- Courts and tribunals
- Insurers

13. INTERNATIONAL TRANSFERS

We may transfer personal data outside Kenya where necessary for the purposes set out in this Policy. Where such a transfer takes place, we ensure that:

- The transfer is made to a jurisdiction with adequate data protection safeguards, or is otherwise permitted under the Data Protection Act, 2019;
- Appropriate contractual and technical protections are put in place with the recipient, including data processing or transfer agreements;
- A transfer risk assessment is conducted where appropriate prior to the transfer.

14. DATA SECURITY

We implement appropriate administrative, technical and physical measures to protect personal data against unauthorised access, alteration, disclosure or destruction, including:

- Encryption of data in transit and at rest, where appropriate
- Access controls and role-based permissions
- Logging and monitoring of system activity
- Incident response procedures
- Regular backups
- Business continuity and disaster recovery arrangements

15. DATA RETENTION

We retain personal data only for as long as necessary to fulfil the purposes for which it was collected, or as required by law. Indicative retention periods are set out below and should be confirmed against the Organisation's Data Retention Schedule:

RECORD	RETENTION PERIOD
Customer contracts	[] years
Recruitment records	[] years
Employee files	[] years
Financial records	[] years
Website logs	[] months

16. YOUR RIGHTS

Subject to applicable law and any exemptions that may apply, you have the following rights in relation to your personal data:

- The right to be informed of the use to which your personal data is to be put;
- The right to access your personal data;
- The right to request correction of inaccurate or incomplete personal data;
- The right to request erasure of personal data, where legally applicable;
- The right to object to certain processing of your personal data;
- The right to withdraw consent, where processing is based on consent;
- The right to request restriction of processing in appropriate circumstances;
- The right to data portability, where applicable.

17. EXERCISING YOUR RIGHTS

To exercise any of the rights set out in this Policy, please contact our Data Protection Officer using the details below:

Email: *[Insert DPO Email]*

Postal Address: *[Insert Address]*

We may need to request specific information from you to verify your identity before responding to your request. We will respond to all legitimate requests within the timeline prescribed under applicable law. If you are not satisfied with our response, you may escalate the matter as set out in Section 23 (Complaints).

18. CHILDREN'S DATA

Where our processing activities involve the personal data of children, we implement additional safeguards, including obtaining parental or guardian consent where required by law and applying appropriate age-verification measures.

19. MARKETING COMMUNICATIONS

Where we process your personal data for direct marketing purposes, we do so on the basis of your consent. You may withdraw your consent and opt out of marketing

communications at any time by using the unsubscribe mechanism provided in our communications, or through our preference centre.

20. THIRD-PARTY WEBSITES

Our website may contain links to third-party websites. This Policy does not extend to any third-party website, and we are not responsible for the privacy practices of third parties. We encourage you to review the privacy policy of any third-party website you visit.

21. CHANGES TO THIS POLICY

We may update this Policy from time to time to reflect changes in our practices or applicable law. Material changes will be notified to you through appropriate channels. The version history and effective date of this Policy are set out in the Document Control section.

22. CONTACT INFORMATION

Organisation: *[Organisation Name]*

Data Protection Officer: *[Insert DPO Name]*

Email: *[Insert Email]*

Telephone: *[Insert Telephone]*

Office: *[Insert Address]*

23. COMPLAINTS

If you believe that your personal data has been processed in a manner that infringes your rights under the Data Protection Act, 2019, you may lodge a complaint with our Data Protection Officer using the contact details set out in Section 22.

You also have the right to lodge a complaint directly with the Office of the Data Protection Commissioner (ODPC), the independent supervisory authority for data protection in Kenya.

INTERNAL USE ONLY — NOT FOR CLIENT-FACING DISTRIBUTION**ANNEX A — IMPLEMENTATION NOTES**

This annex accompanies the template for internal and client use and must be removed before the Policy is published or issued in final form.

Mandatory Clauses

Sections 1 (Introduction), 2 (Scope), 4 (Who We Are), 16 (Your Rights), 22 (Contact Information) and 23 (Complaints) are mandatory in every Privacy Policy issued using this template, regardless of the client's sector or processing activities.

Organisation-Specific Sections

Sections 5 (Information We Collect), 6 (Sources of Personal Data), 7 (Purposes of Processing), 12 (Data Sharing), 13 (International Transfers) and 15 (Data Retention) must be populated with information specific to the client's actual processing activities. Generic or template language should never be retained in these sections in the final published Policy.

When Specialist Legal Review Is Recommended

- The client processes AI systems that inform or make decisions affecting individuals (Sections 10 and 11);
- The client processes health, biometric or other special category data at scale (Section 5);
- The client transfers personal data outside Kenya on a regular or systematic basis (Section 13);
- The client operates in a regulated sector with sector-specific data protection guidance (e.g. banking, insurance, telecommunications, health);
- The client's processing involves children's data at scale (Section 18).

Supporting Documents Checklist

Before finalising a client-specific Policy from this template, confirm that the following supporting documents exist or are being developed in parallel:

- Data Retention Schedule
- Cookie Inventory
- Records of Processing Activities (ROPA)
- Data Processing Agreements with third-party processors
- AI Governance Policy (where AI systems are in use)
- Data Breach Response Plan

Reference: Muchangi Patrick & Associates Advocates — Template Library. This annex should be deleted from the document before delivery of the final Privacy Policy to any client or publication on a client's website.