Data Protection Policy

MELANIN KAPITAL LIMITED

Note about this policy template: Lots of template policies are unhelpfully long and simply reiterate large portions of the legislation. This template is different: it aims to provide a concise and practical document that can be used by small organisations as the foundation for a working Data Protection Policy. If you have any doubt about your legal obligations, you should always check with a lawyer.

Last updated	30TH MARCH 2023

Definitions

Organisation	means MELANIN KAPITAL LIMITED, a company registered under number [company number, if applicable].
DPA	means the TheDataProtectionAct which implements the Kenya General Data Protection Regulation.
Responsible Person	means [CDO-Herein Chief Data Officer-] [CEO and Co-Founder]
Register of Systems	means a register of all systems or contexts in which personal data is processed by the Organisation.

INTRODUCTION

In the recent years, information has increasingly become a critical resource that has to be managed carefully. Generally, much of today's information consists of personal data relating to individuals. The Data Protection Act, 2019 came into effect on 25th November, 2019. It gives effect to Article 31 of the Constitution which safeguards the right to privacy and guarantees the privacy of communications. It is modelled on the Principles set out in the European Union (EU) General Data Protection Regulation (GDPR).

The overall aim of the Act is to protect personal data. The Act establishes the office of the Data Protection Commissioner (DPR) which shall oversee the implementation and enforcement of the Act. Appointment of the Data Protection Commissioner is still pending.

The Act provides for:

a) The principles for data processing to be observed by data processors and controllers

b) The rights of data subjects.

c) Penalties for non-compliance

2. PURPOSE

Data protection policy informs the Organization on the management of Personal Data in the information life cycle and the commitment of the Organization to protect the Personal Data including the Personal Sensitive Data. The purpose of this policy document is to ensure effective protection and management of Personal Data by identifying, assessing, monitoring and mitigating privacy risks in programs and activities involving the collection, retention, use, disclosure and disposal of Personal Data;

Lawful purposes

All data processed by the Organisation must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task, or legitimate interests.

The Organisation shall note the appropriate lawful basis in the Register of Systems.

Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.

Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Organisation's systems.

This policy therefore seeks to:

• Ensure clarity about how personal data must be processed and the Organization's expectations for all those who process personal data on its behalf.

• Ensure compliance with the data protection law and with good practice;

• Protect the Organization's reputation by ensuring the personal data entrusted to the Organization is processed in accordance with data subjects' rights

• Protect the Organization from risks of personal data breaches and other breaches of data protection law.

SCOPE

This policy applies to all data subjects whose data is or has been collected or processed by the Organization and or contracted third parties. The same shall be the overarching guiding policy in relation to matters of Privacy and Data Protection and sets out the requirements for the protection of Personal Data in manual, electronic or any other form.

2. Data protection principles

The Organisation is committed to processing data in accordance with its responsibilities under the DPA.

DPA requires that personal data shall be:

processed lawfully, fairly and in a transparent manner in relation to individuals.

collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be incompatible with the initial purposes.

adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay.

kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the DPA in order to safeguard the rights and freedoms of individuals; and

processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against

accidental loss, destruction, or damage, using appropriate technical or organisational measures."

2. General provisions

This policy applies to all personal data processed by the Organisation.

The Responsible Person shall take responsibility for the Organisation's ongoing compliance with this policy.

This policy shall be reviewed at least annually.

The Organisation shall register with the Information Commissioner's Office as an organisation that processes personal data.

3. Lawful, fair, and transparent processing

To ensure its processing of data is lawful, fair, and transparent, the Organisation shall maintain a Register of Systems.

The Register of Systems shall be reviewed at least annually.

Individuals have the right to access their personal data and any such requests made to the Organisation shall be dealt with in a timely manner.

4.

5. Data minimisation

The Organisation shall ensure that personal data are adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

GOVERNANCE

4.1 Policy Dissemination and Enforcement

The Organization must ensure that all Organization employees are aware of and comply with the contents of this policy. In addition, the Organization will make sure all Third Parties engaged to process Personal Data on Organization's behalf (i.e. their Data Processors) are aware of and comply with the contents of this policy. Commitment to such compliance must be obtained from all Third Parties (in written form, via clauses or contractual obligations), whether companies or individuals, prior to granting them access to Personal Data controlled by the Organization.

2 Data Protection by Design To ensure that all Data Protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each of them must go through a risk assessment followed by an approval process based on the risk assessment results, before commencement. The Organization must ensure that a Data Protection Assessment is conducted proactively for all new and/or revised systems or processes for which it has responsibility.

The Organization should also carry out an impact assessment of the envisaged processing operations on the protection of personal data prior to personal data processing where a data processing operation is likely to result in a high risk to the rights and freedoms of a data subject by virtue of its nature, scope, context and purposes.

The Organization should consult with a Data Protection subject matter expert and representatives from Compliance, Legal and ICT, during the course of completing the assessment. The subsequent findings must then be submitted for review and approval. Where applicable, the Information & Communications Technology (ICT) department, as part of its IT system and application design review process, will cooperate with the Data Protection subject matter expert to assess the impact of any new technology uses on the security of Personal Data.

Compliance Monitoring

To confirm that an adequate level of compliance is being achieved by the Organization in relation to this policy, the Organization will carry out an annual Data Protection compliance audit. Each audit will, at a minimum, assess compliance to this policy and the operational practices in relation to the protection of Personal Data, including:

- Assignment of responsibilities
- Raising awareness
- Training of Employees
- Adequacy of organizational and technical controls to protect Personal Data
- Records management procedures (including data minimization)
- Adherence to the qualified rights of the Data Subject
- Privacy by Design and Default
- Consent for direct marketing
- Personal Data transfers
- Personal Data incident management (including Personal Data breaches)
- Personal Data complaints handling
- Currency of Data Protection policies and Privacy Notices
- Accuracy of Personal Data being stored
- Conformity of Data Processor activities
- Adequacy of procedures for redressing poor compliance

6. Accuracy

The Organisation shall take reasonable steps to ensure personal data is accurate.

Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

[Add considerations relevant to the Organisation's particular systems]

7. Record Keeping/Archiving / removal

To ensure that personal data is kept for no longer than necessary, the Organisation shall put in place an archiving policy for each area in which personal data is processed and review this process annually.

The archiving policy shall consider what data should/must be retained, for how long, and why.

Personal data shall only be retained for as long as it is reasonably necessary to satisfy the purpose for which it is processed unless the retention is:

required or authorized by law;

reasonably necessary for a lawful purpose;

authorized or consented by the data subject; or

for historical, statistical or research purposes.

8. Security

RIGHTS OF A DATA SUBJECT

A data subject has the following rights:

- To be informed of the use of their personal data.
- To have access to their personal data in the Organization's custody.
- To give consent before data is processed.
- To have inaccurate/incorrect data corrected or deleted.
- To object to collection or processing of all or part of personal data.
- To withdraw consent to the processing of their personal data. Withdrawal shall however not affect the lawfulness of processing based on prior consent before the withdrawal.
- To be protected from automatic data processing that significantly affects them.
- To upon request, receive their personal data in a structured, commonly used, and machine-readable format.

The Organisation shall ensure that personal data is stored securely using modern software that is kept-up to date.

Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.

When personal data is deleted, this should be done safely such that the data is irrecoverable.

Appropriate back-up and disaster recovery solutions shall be in place.

PRINCIPLE	DEFINITION
Lawfulness, Fairness and Transparency	Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. The Organization must tell the Data Subject what Processing will occur, through Terms and Conditions, the Processing must match the description given to the Data Subject and it must be for one of the purposes specified in the applicable Data Protection regulation.
Purpose Limitation	Personal Data shall be collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes. This means the Organization must specify exactly what the Personal Data collected will be used for and limit the Processing of that Personal Data to only what is necessary to meet the specified purpose.
Data Minimisation	Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed. This means the Organization must not store any Personal Data beyond what is strictly required.
Accuracy	Personal Data shall be accurate and kept up to date. This means the Organization must have in place processes for identifying and addressing outof-date, incorrect and redundant Personal Data.
Storage Limitation	Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary

	for the purposes for which the Personal Data is Processed, in line with legal and regulatory requirements. This means the Organization must, wherever possible, store Personal Data in a way that limits or prevents identification of the Data Subject.
. Integrity & Confidentiality	Personal Data shall be Processed in a manner that ensures appropriate security of the Personal Data, including reasonable protection against unauthorised or unlawful Processing, and against accidental loss, destruction or damage. The Organization must use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data are maintained at all times.

ORGANIZATION OBLIGATIONS.

1). To ensure its processing of data is lawful, fair and transparent, the Organization shall maintain a register of Systems which shall be reviewed at least annually. The register of Systems shall include the appropriate lawful basis of collecting/processing data.

2). The Organization shall provide for Individuals to access their personal data and any such requests made to the Organization shall be dealt with in a timely manner.

3). All data processed by the Organization must be done on one of the following lawful basis:

a. consent,

b. contract,

c. legal obligation, or

d. legitimate interests under approval of regulatory body

4) Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be securely kept with the personal data.

5) Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Organization's systems.

6) The Organization shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

7) The Organization shall take reasonable steps to ensure personal data is accurate. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

8) To ensure that personal data is not kept for longer than necessary, the Organization shall put in place archiving guidelines for each area in which personal data is processed and review this process annually. The archiving guidelines shall consider what data should/must be retained, for how long, and why.

9) Access to personal data shall be limited to personnel who need access and appropriate security measures shall be put in place to avoid unauthorized sharing of information. Where personal data is deleted, this shall be done in a manner that the data is irrecoverable.

Accountability

The team assigned the Data Controller role shall be responsible for, and be able to demonstrate, compliance. This means the Organization must demonstrate that the six Data Protection Principles (outlined above) are met for all Personal Data for which it is responsible.

Data Collection, Retention & Transfer

Personal Data should not be processed unless one of the following applies:

The data subject consents to the processing for one or more specified purposes.

• The nature of the business purpose necessitates collection of the Personal Data from other persons or bodies.

• For the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract.

• For compliance with any legal obligation to which the controller is subject.

• In order to protect the vital interests of the data subject or another person.

• For the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

For the legitimate interests pursued by the data controller or data processor by a third party to whom the data is disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject.

• For the purpose of historical, statistical or scientific research.

• The nature of the business purpose necessitates collection of the Personal Data from other persons or bodies.

• The collection must be carried out under emergency circumstances in order to protect the vital interests of the Data Subject or to prevent serious loss or injury to another person. • If Personal Data is collected from someone other than the Data Subject, the Data Subject must be informed of the collection unless one of the following apply:

the Data Subject has received the required information by other means

the information must remain confidential due to a professional secrecy obligation

a national law expressly provides for the collection, Processing or transfer of the Personal Data.

Where it has been determined that notification to a Data Subject is required, notification should occur promptly, but in no case later than one month unless otherwise stated by applicable laws or regulations

• Any category of sensitive personal data shall not be processed unless the processing is in line with the above parameters.

Transfer

As a principle, personal data shall not be transferred outside Kenya. However, personal data may be transferred to another country in the following instances for the purpose of 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.

There is adequate proof of adequate data protection laws by the recipient country.

where the Organization has proved to the relevant authorities that there are appropriate safeguards with respect to the security and protection of the personal data;

where the data subject has given explicit consent to the proposed transfer, after having been informed of the possible risks of the transfer;

where the transfer is necessary for performance of contractual obligations;

for any matter of public interest;

for the establishment, exercise or defence of a legal claim;

in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data, the Organization shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the relevant stakeholders as prescribed by statutory and/or regulatory requirements. Where there is a breach of security of personal data or there is reasonable ground to believe personal data has been accessed or acquired by an unauthorized person, the breach shall be reported within the prescribed period to the relevant authorities. The Organization shall also communicate the breach to the data subject in the prescribed manner, unless the identity of the data subject cannot be established. However, notification of the breach to the data subject may be delayed for purposes of prevention, detection or investigation of offences by the relevant authorities.

8. **EXEMPTIONS.**

The processing of personal data is exempt from the provisions of this Act if—

(a) It relates to processing of personal data by an individual in the course of a purely personal or household activity;

(b) If it is necessary for national security or public interest; or disclosure is required by or under any written law or by an order of the court.

9. **REVIEW**

This policy shall be reviewed every five years or earlier upon change of regulations or the Organization's operating conditions.

END OF POLICY

For more resources visit https://www.odpc.go.ke/

https://melaninkapital.com