A Data Protection Guide for Small and Medium-sized Enterprises (SMEs) in Kenya"

Strathmore University

Centre for Intellectual Property and Information Technology Law

Introduction

Parliament passed the Data Protection Act of 2019 (The Act) to give effect to the Right to Privacy for all individuals as provided for under the Constitution of Kenya 2010. This Act seeks to ensure that the privacy of Kenyan citizens is protected. It is a major development in Kenya that will require significant changes to the operations of private and public entities.

Personal data Sensitive data is data making known a person's features such as race, health status, ethnicity, social origin, religious beliefs biometric data, property details, marital status, family information including names of their children, parents, spouse or spouses, sex or their sexual orientation.

The aim of this pamphlet is to assist you to understand your obligations under the Act as a Small and Medium Enterprise (SME) in ensuring the protection of personal data in your day to day business operations.

Does it apply to you?

The Act applies to all SMEs that collect, control and process personal data as part of the core business. Therefore, if you collect, control or process personal data, you are required to be compliant with the provisions of this Act.

- **A Data Controller** determines the use and method of processing of personal data
- **A Data Processor** processes (e.g., collects or analyzes) personal data on behalf of the data controller.
- **The Data Commissioner** will set a minimum threshold for registration – if you exceed the threshold, you will need to register with the office of the Data Protection Commissioner.

Principles for the collection and processing of personal data

The Act outlines the following principles and SME's should understand and comply with these as outlined.

01 Respect for the right to privacy

You are required to respect every individual's right to privacy. The Constitution of Kenyan states that privacy includes four duties:

- Refraining from searching the person or home of anyone;
- Not seizing people's possessions;
- Avoiding revealing or requiring the submission of information regarding the family or private affairs of persons; or
- Not infringing a person's communications.

With respect to data, the Data Protection Act implements these rights.

02 Clear, lawful and valid reasons for collection

Collection of personal data must be done for clear, lawful and valid reasons. You must make it clear why you are collecting or processing an individual's data. The Act defines a data subject as any individual, whose personal data is being collected, held or processed.

03 Legal, fair and transparent processing

You are to make available all information relating to the processing and control of the data collected, at all times. This information must be clear, easily understandable and accessible if requested.

04 Collection and processing of only relevant data

You are to collect and process only relevant data, this being the data necessary for the performance of your obligations to the data subject. Processing of personal data is limited to the reasons for its collection.

05 Accurate and up to date data

You are to ensure that the data you collect is accurate and up to date. Where the data is incorrect, a data subject may ask you to correct it or delete it. You are to correct or delete it upon their request.

06 Length and safety of stored data

You are to properly and safely dispose of the personal data, once processing is complete, as you must not hold it for longer than necessary. You are also required to inform the data subject of the length of time you intend to store their data. Finally, you must ensure that this personal data is kept safe.

07 Transfer of data outside Kenya

If you wish to transfer personal data outside Kenya, you must ensure that all necessary safeguards are met by the receiver of this data. The safeguards must be secure and suitable for the protection of personal data. The data subject must also be informed and their consent given for such a transfer to be legal. Consent may be verbal, written, implied or electronically logged.

Registration of Controllers and Processors

The Act provides for an Office of the Data Protection Commissioner, that is a state office. If you are a Data Controller or Processor, you will have to be registered and licensed by the Data Protection Commissioner, who will prescribe criteria to be met for registration. Once you register and meet the criteria, you get a certificate that will require periodic renewal.

Collection of personal data

The Act is concerned with the collection of personal data; information relating to an identified natural individual. Collection of this information may be direct or indirect. Where direct it is collected from the data subject and where indirect it is collected for example, from public data, where the data subject has consented to the collection of their personal source from another source.

Where an individual has consented to collection of their data, you are legally allowed to collect such data. Where they cannot consent to collection of their personal data, such as in the case of a child, a legal guardian can consent on their behalf.

What are the data subject's rights?

The Act lists the following as rights to the data subjects:

Right to be informed of the use of the data acquired

When collecting personal data, you must inform the data subject why you are collecting and processing their data. You must give clear, lawful and valid reasons for the collection and processing of their data.

Right to access collected data

A data subject is allowed to access their personal data in your possession at all times, upon request. You are required to facilitate their access at reasonable speed.

Right to object to the processing of all of their personal data

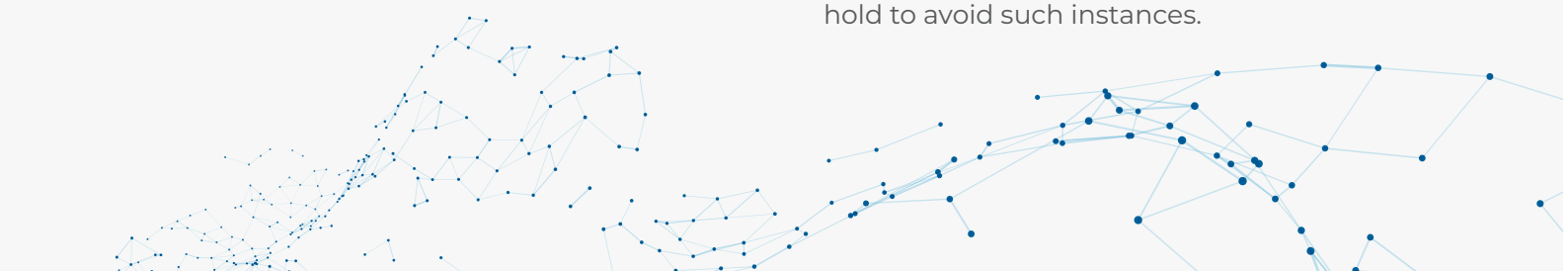
A data subject may choose to stop you from processing their personal data. You are required to stop processing immediately, as further processing will be without their permission and it will be illegal.

Right to ask for correction of false or misleading data

Upon the request of a data subject, you are required to correct incorrect or false personal data in regards to the data subject. You are to correct the incorrect data as soon as possible at no expense to the data subject.

Right have deleted false or misleading data about them

You are required to delete any false, misleading or incorrect information about the data subject, upon their request. This will require that you frequently update personal data you hold to avoid such instances.



SME's duty to Notify

Where practicable, you must tell the data subject the following;

- Their rights under the Data Protection Act 2019.
- The fact that their data is being collected and the reasons why.
- All third parties that you intend to transfer their data to and for what purpose.
- Your key contacts and platforms for communication.
- A detailed breakdown of your technical and organizational security measures made to protect the data collected.
- The kind of data collected voluntarily or mandatorily collected as per the law.
- Impact to a data subject for failing to provide all or any part of their requested data.

Where there has been an unauthorised access of personal data under your protection (breach), you are required to inform the Data Protection Commissioner of the breach in writing within 72 hours of it happening. Past 72 hours you are to attach the notification of breach with reasons explaining the delay in notification.

Data Protection Impact Assessment (DPIA)

Where the processing of personal data is risky and highly likely to result in breach, you will in partnership with the Data Protection Commissioner, carry out a Data Protection Impact Assessment. The DPIA will assess the measures set out to protect personal data that you hold.

The office of the Data Protection Commissioner will issue directives on how to conduct DPIAs.

Conditions of Consent

You must prove that consent for the collection and processing of personal data was given to you by the data subject. The Act also provides that at any point, the data subject may withdraw their consent, thus making the processing after the withdrawal illegal. You are to obtain consent without the use of force, trickery, or manipulation. Some narrow alternatives to consent are provided in the Act.

Personal data relating to children

Where a child is the data subject, consent to collect and process their data is given by their parents or legal guardian as the child cannot give their consent. As a data controller or processor you are required to set measures in place to establish the age of a data subject. This can be achieved through the request of legal identification. There may be some exceptions to this. For example, those offering counselling services may be allowed to collect and process children's personal data without the consent of the parents or guardians.

Automated Processing

During processing of personal data you must ensure that the whole process is not left to fully automated software, systems or tools. You are required to ensure that there is human decision making as part of the processing system as the Act requires that an automated system is to be complimented by human decision making. Thus fully autonomous automated systems in processing personal data are generally not allowed.

Data Protection Officers

Depending on your capacity, SME's may choose to have a Data Protection Officer (DPO), however this is not a mandatory requirement under the Act. Given the complexities of data protection, and depending on your particular industry or sector, it may be advisable to seek the services of a full- or part-time DPO.

Commercialized data

You can only commercialize data upon receiving consent from the data subject. You are required to fully inform the Data subject in clear terms of your intention to commercialize the data. Having this information they must then give their consent to this processing and commercialization. The act requires that commercialized personal data is anonymized which requires the removal of personal identifiers such as names, addresses, postcode, telephone number, photograph or image such that it no longer identifies the data subject.

When can you transfer Personal Data outside Kenya

For you to transfer data outside Kenya, you must provide proof to the Office of the Data Protection Commissioner of sufficient measures with regards to the security and protection of personal data that you hold. You must also provide the receiver's data protection laws and safeguards. Where satisfied by the safeguards the Data Protection Commissioner shall allow you to transfer the data.

How will the act be enforced?

Any wronged data subject may file a complaint against a data controller or processor, to the Data Protection Commissioner who then upon receiving the complaint shall begin an investigation within 90 days. Where the Data Protection Commissioner finds breach of a binding provision of the Act, s/he may issue an enforcement notice.

Upon further investigation, where found guilty, the Data Protection Commissioner may impose a penalty of up to five million shillings or one percent of the data controller or processor's turnover in the case of an undertaking, whichever is lower. If the data controller or processor is unhappy with the enforcement notice or penalty notice, they may contest it in the High Court.

Conclusion

Given the increasing importance of the protection of personal data both globally and in Kenya, the Act provides key obligations that will ensure the right to privacy is enforced, including by SMEs. It is important for SMEs to consider compliance with the provisions of this act from the earliest moment, especially where they collect, control, or process personal data.

GET IN TOUCH WITH US!

CIPIT is a research and training centre at Strathmore University. This pamphlet is intended only as an initial introduction to the Data Protection Act - the implications of the Act are wide and extensive, and cannot be fully explained in a brief publication. We are available to help you understand the law and how it applies to you. Please contact us if you have any questions about this pamphlet, or visit our website for more resources.

+254 (0) 703 034 612 cipit@strathmore.edu

This pamphlet does not contain legal advice. If you have a question regarding your specific situation, please consult a data protection lawyer or get in touch with us.