DATA PROTECTION LAWS OF THE WORLD

Kenya

KENYA

Last modified 12 January 2023

LAW

The Data Protection Act, 2019 (the "**Act**") came into force on 25th November, 2019 and is now the primary statute on data protection in Kenya. It gives effect to Article 31 c) and d) of the Constitution of Kenya, 2010 (right to privacy).

In October 2020, by virtue of the powers conferred to him under the Act, the Cabinet Secretary for Information, Communication, Technology, Innovation and Youth Affairs gazetted the Data Protection (Civil Registration) Regulations, 2020 (the "**Regulations**"). The Regulations apply to civil registries involved in processing personal data for registrations such as births, deaths, adoptions, persons, passports and marriages.

Since the Data Protection Commissioner's (DPC) appointment on 16 November 2020, significant efforts have been made in developing regulations for the implementation of the Act.

- **Data Protection (Compliance & Enforcement) Regulation, 2021** – sets out the complaints handling procedures and enforcement mechanisms in the event of non-compliance with the provisions of the Act;

- **Data Protection (Registration of Data Controllers & Data Processors) Regulations, 2021** – provides for the registration of data controllers and data processors with the DPC. The threshold for mandatory registration is also set out under these regulations; and

- **Data Protection (General) Regulations, 2021** – elaborates in more detail the rights of data subjects, restrictions on commercial use of personal data, duties and obligations of data controllers and data processors, elements of implementing data protection by design or default, notification of personal data breaches, transfer of personal data outside Kenya, conduct of data protection impact assessment and other general provisions.

The above regulations were gazetted in January and came into effect on 14 February 2022 with the exception of the Data Protection (Registration of Data Controllers & Data Processors) Regulations, 2021 which came into force on 14 July 2022.

The DPC has also issued a number of guidelines, these include:

- **Guidance Note on Registration of Data Controllers and Data Processors** - developed to assist entities in ascertaining if they are data controllers or data processors, and to understand their obligations with respect to mandatory registration;
- **Guidance Note on Processing Personal Data for Electoral Purposes** - developed to assist data controllers and data processors dealing with voters' personal data and members of political parties' personal data to understand their obligations under the Act;
- **Guidance Note on Data Protection Impact Assessment** - to assist data controllers and data processors to understand their obligations under the Act and the need to undertake a Data Protection Impact Assessment; and
- **Guidance Note on Consent** - developed to assist data controllers and data processors to understand their duties

under the Act and their obligations as far as obtaining consent is concerned.

The DPC has also published a **Complaints Management Manual** which sets out the complaints management handling procedure by the DPC; and the **Alternative Disputes Resolution Framework** which provides guidance to stakeholders who wish to engage in Alternative Dispute Resolution (ADR) to resolve their disputes arising under the Act.

DEFINITIONS

Definition of personal data

Section 2 of the Act

Personal data is defined as data relating to an identified or identifiable natural person.

Definition of sensitive personal data

Section 2 of the Act

Sensitive personal data is defined as data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject.

NATIONAL DATA PROTECTION AUTHORITY

Part II of the Act

The Act established the Office of the Data Protection Commissioner (DPC) whose mandate includes overseeing the implementation and enforcement of the provisions of the Act. The DPC is also tasked with the maintenance of the register of data controllers and processors, receiving and investigation of complaints under the Act and carrying out inspections of public and private entities to evaluate the processing of personal data.

REGISTRATION

Section 18 of the Act

Data processors and data controllers are required to be registered with the DPC. The DPC, however, has discretion to prescribe the thresholds for mandatory registration based on:

- the nature of industry;
- the volumes of data processed; and
- whether sensitive personal data is being processed.

The Data Protection (Registration of Data Controllers & Data Processors) Regulations, 2021, provides for the registration of data controllers and data processors with the DPC. The threshold for mandatory registration is also set out under these regulations. The DPC also launched a portal where applications for registration are submitted in the prescribed form and upon payment of a prescribed fee. Where the DPC is satisfied that the applicant has fulfilled the requirements for registration, a certificate of registration is issued within 14 days and entry of the applicant's details is made in the register of data controllers and data processors.

The certificate of registration issued is valid for 24 months from the date of issuance.

A data controller or data processor with an annual turnover or revenue of below Kenya Shillings Five Million (approx. USD 40,000) and has less than 10 employees is exempt from mandatory registration.

Data controllers and data processors who process data for the following purposes regardless of their annual turnover or revenue or number of employees have to be registered under the Regulations:

- canvassing political support among the electorate;
- crime prevention and prosecution of offenders (including operating security CCTV systems);
- gambling;
- operating an educational institution;
- health administration and provision of patient care;
- hospitality industry firms, excluding tour guides;
- property management including the selling of land;
- provision of financial services;
- telecommunications network or service providers;
- businesses that are wholly or mainly in direct marketing; and
- transport services firms (including online passenger hailing applications); and businesses that process genetic data.

DATA PROTECTION OFFICERS

Section 24 of the Act

The Act makes provisions for the designation of Data Protection Officers (DPOs) but this obligation is not mandatory.

DPOs can be members of staff and may perform other roles in addition to their roles. A group of entities can share a DPO and the contact details of the DPO must be published on the organisation's website and communicated to the DPC.

DPOs have the following roles:

- advising the data controller or data processor and their employees on data processing requirements provided under the Act or any other written law;
- ensuring compliance with the Act;
- facilitating capacity building of staff involved in data processing operations;
- providing advice on data protection impact assessment; and
- co-operating with the DPC and any other authority on matters relating to data protection.

DPO's under the Regulations also have the following additional roles:

- monitoring and evaluating the efficiency of the data systems in the organization; and
- keeping written records of the processing activities of the civil registration entity.

COLLECTION & PROCESSING

Section 25 of the Act

The processing of personal data must comply with the principles prescribed in this part. It must be:

- processed in accordance with the right to privacy of the data subject;
- processed lawfully, fairly and in a transparent manner in relation to any data subject;
- collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;
- adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;
- collected only where a valid explanation is provided whenever information relating to family or private affairs is required;
- accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay;
- kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and
- not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject.

Section 30 of the Act

The Act recommends personal data to be collected and processed lawfully. The lawful reasons for processing include:

a. Consent of the data subject; or
b. the processing is necessary:
    a. 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;
    b. for compliance with any legal obligation to which the controller is subject;
    c. in order to protect the vital interests of the data subject or another natural person;
    d. for the performance of a task carried out in the public interest or in the exercise of
        - official authority vested in the controller;
        - the performance of any task carried out by a public authority;
    e. for the exercise, by any person in the public interest, of any other functions of a public nature;
    f. 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; or
    g. for the purpose of historical, statistical, journalistic, literature and art or scientific research.

It is an offence to process personal data without a lawful reason.

Under the Regulations civil registration entities must ensure that they collect only personal data permitted by the data subject and that the appropriate steps are taken to ensure the quality and security of the personal data.

Where the registries intend to use such data for another purpose, they must either ensure that the purpose is compatible with the initial purpose or, where that is not the case, seek fresh consent.

The Data Protection (General) Regulations, 2021 elaborate in more detail restrictions on commercial use of personal data, duties and obligations of data controllers and data processors, elements of implementing data protection by design or default, conduct of data protection impact assessment and other general provisions.

TRANSFER

Part VI of the Act

The transfer of personal data outside Kenya is highly regulated under the Act. Prior to any transfer the data controller or data processor must provide proof to the DPC on the appropriate safeguards with respect to the security and protection of the personal data including jurisdictions with similar data protection laws.

The consent of the data subject is required for the transfer of sensitive personal data out of Kenya.

Under the Regulations, civil registration registries cannot transfer personal data collected for civil registration purposes outside Kenya without the written approval of the DPC.

The Data Protection (General) Regulations, 2021 elaborate in more detail transfer of personal data outside Kenya. The Regulations provide for 4 legal bases for the transfer of personal data out of the country which include;

a. appropriate data protection safeguards in the country or territory where recipient is based in;
b. adequacy: an adequacy decision made by the DPC that the country, territory or the international organization where data is being transferred ensures an adequate level of protection of personal data;
c. necessity: transfer is deemed to be necessary if it is:
    a. 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;
    b. for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person;
    c. for any matter of public interest;
    d. 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;

e. 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.

d. consent of the data subject on the condition they have consented to the proposed transfer and have been informed of the possible risks of transfer.

SECURITY

Sections 41 and 42 of the Act

Data controllers and processors are required to implement the appropriate organizational and technical measures to implement data protection principles in an effective manner.

Civil registration registries are mandated to formulate written data security procedures which must include the following:

- instructions concerning physical protection of the database sites and their surroundings;
- access authorizations to the database and database systems;
- description of the means intended to protect the database systems and the manner of their operation for this purpose;
- instructions to authorized officer of the database and database systems regarding the protection of data stored in the database;
- the risks to which the data in the database is exposed in the course of the civil registration entity's ongoing activities;
- the manner of dealing with information security incidents, according to the severity of the incident;
- instructions concerning the management and usage of portable devices;
- instructions with respect to conducting periodical audits to ensure that appropriate security measures, in accordance with the Procedure and these Regulations exist; and
- instructions regarding backup of personal data.

As far as technical measures are concerned, the Regulations require the use of hashing and cryptography to limit the possibility of repurposing personal data. The Regulations also require that the contract between a data controller and a data processor to include a clause on security measures subjecting the data processor to appropriate technical and organizational measures in relation to keeping personal data secure.

With respect to organizational measures, the Regulations require a data controller or data processor to develop, publish and regularly update a policy reflecting their personal data handling practices. The policy may include:

a. the nature of personal data collected and held;
b. how a data subject may access their personal data and exercise their rights in respect to that personal data;
c. complaints handling mechanisms;
d. lawful purpose for processing personal data;
e. obligations or requirements where personal data is to be transferred outside the country, to third parties, or other data controllers or data processors located outside Kenya and where possible, specify such recipients;
f. the retention period and schedule; and
g. the collection of personal data from children, and the criteria to be applied.

The Regulations provide for specific obligations to the data controller and data processor under the data protection principle of integrity, confidentiality and availability. These include:

a. having an operative means of managing policies and procedures for information security;
b. assessing the risks against the security of personal data and putting in place measures to counter identified risks;
c. processing that is robust to withstand changes, regulatory demands, incidents, and cyber-attacks;
d. ensuring only authorised personnel have access to the data necessary for their processing tasks;
e. securing transfers shall be secured against unauthorised access and changes;
f. securing data storage from use, unauthorised access and alterations;

g. keeping back-ups and logs to the extent necessary for information security;
h. using audit trails and event monitoring as a routine security control;
i. protecting sensitive personal data with adequate measures and, where possible, kept separate from the rest of the personal data;
j. having in place routines and procedures to detect, handle, report, and learn from data breaches; and
k. regularly reviewing and testing software to uncover vulnerabilities of the systems supporting the processing.

BREACH NOTIFICATION

Breach Notification

Section 43 of the Act

As far as technical measures are concerned, the Regulations require the use of hashing and cryptography to limit the possibility of repurposing personal data. The Regulations also require that the contract between a data controller and a data processor to include a clause on security measures subjecting the data processor to appropriate technical and organizational measures in relation to keeping personal data secure.

With respect to organizational measures, the Regulations require a data controller or data processor to develop, publish and regularly update a policy reflecting their personal data handling practices. The policy may include:

a. the nature of personal data collected and held;
b. how a data subject may access their personal data and exercise their rights in respect to that personal data;
c. complaints handling mechanisms;
d. lawful purpose for processing personal data;
e. obligations or requirements where personal data is to be transferred outside the country, to third parties, or other data controllers or data processors located outside Kenya and where possible, specify such recipients;
f. the retention period and schedule; and
g. the collection of personal data from children, and the criteria to be applied.

The Regulations provide for specific obligations to the data controller and data processor under the data protection principle of integrity, confidentiality and availability. These include:

a. having an operative means of managing policies and procedures for information security;
b. assessing the risks against the security of personal data and putting in place measures to counter identified risks;
c. processing that is robust to withstand changes, regulatory demands, incidents, and cyber-attacks;
d. ensuring only authorised personnel have access to the data necessary for their processing tasks;
e. securing transfers shall be secured against unauthorised access and changes;
f. securing data storage from use, unauthorised access and alterations;
g. keeping back-ups and logs to the extent necessary for information security;
h. using audit trails and event monitoring as a routine security control;
i. protecting sensitive personal data with adequate measures and, where possible, kept separate from the rest of the personal data;
j. having in place routines and procedures to detect, handle, report, and learn from data breaches; and
k. regularly reviewing and testing software to uncover vulnerabilities of the systems supporting the processing.

Mandatory Breach Notification

Yes. Please see above analysis under "Breach Notification".

ENFORCEMENT

The DPC has the duty to ensure the implementation and enforcement of the Act.

The Data Protection (Compliance & Enforcement) Regulation, 2021 sets out the complaints handling procedures and enforcement mechanisms in the event of non-compliance with the provisions of the Act. The Regulations provide for the process and procedure of lodging of complaints with the DPC.

The DPC is also required to maintain an up-to-date register of complaints stating the particulars of the complainant and complaint.

Section 62 of the Act

In instances where the DPC is satisfied that any person has violated the provisions of the Act, he has the power to issue penalty notices for up to a maximum of Kenya Shillings Five Million (approximately USD 50,000) or 1% of an undertaking's annual turnover the preceding year, whichever is lower.

In addition, any act which constitutes an offence under the Act where a penalty is not provided attracts a fine of up to Kenya Shillings Three Million (approx. USD 30,000) or imprisonment for up to 10 years or both a fine and imprisonment.

Under the Data Protection (Compliance & Enforcement) Regulations, 2021 the DPC has the power to issue an enforcement notice where a person fails to comply with the provisions of the Act or the Regulations. A penalty notice is issued where there is failure to comply with the enforcement notice. The penalty notice will contain the reasons why the DPC is imposing a penalty, the administrative fine imposed, how the fine is to be paid and the rights of appeal the decision. The DPC may impose a daily fine of not more than Ksh. 10,000 (approx. USD 100/-) for each penalty identified, until the breach is rectified.

ELECTRONIC MARKETING

Section 37 of the Act

The use of personal data for commercial purposes is prohibited unless the person undertaking this processing:

- has sought and obtained express consent from a data subject; or
- is authorized to do so under any written law and the data subject has been informed of such use when collecting the data from the data subject.

The General Regulations states that a data controller or data processor is considered to be using personal data for commercial purposes if the personal data of a data subject is used to advance commercial or economic interests, including inducing another person to buy, rent, lease, join, subscribe to, provide or exchange products, property, information or services, or enabling or effecting, directly or indirectly, a commercial transaction.

The Regulations further includes circumstances where the personal data is used for direct marketing through:

a. sending of a catalogue through any medium addressed to a data subject;
b. displaying an advertisement on an online media site where a data subject is logged on using their personal data; or
c. sending an electronic message to a data subject about a sale, or other advertising material relating to a sale, using personal data provided by a data subject.

An exception to direct marketing restrictions is provided where the personal data is not used or disclosed to identify or target a particular recipient.

Personal data other than sensitive personal data is only permitted to be used for direct marketing where:

a. the data controller or data processor has collected the personal data directly from the data subject;
b. a data subject is notified that direct marketing is one of the purposes for which personal data is collected;
c. the data subject has consented to the use or disclosure of the personal data for the purpose of direct marketing;
d. the data controller or data processor provides a simplified opt-out mechanism for the data subject to request not to

receive direct marketing communications; or

e. the data subject has not made an opt-out request.

The Cabinet Secretary in charge of information, communication and technology may, in consultation with the DPC, develop guidelines on the commercial use of personal data.

ONLINE PRIVACY

Kenyan law does not regulate online privacy. The Regulations have not prescribed any requirements or guidelines in regulating online privacy.

KEY CONTACTS

IKM Advocates
www.dlapiperafrica.com/en/kenya/

William Maema
Partner
IKM Advocates
T +254 20 2773 000
wmaema@ikm.co.ke

Imelda Anika
Senior Associate
IKM Advocates
T +254 722 898 393
ianika@ikm.co.ke

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.