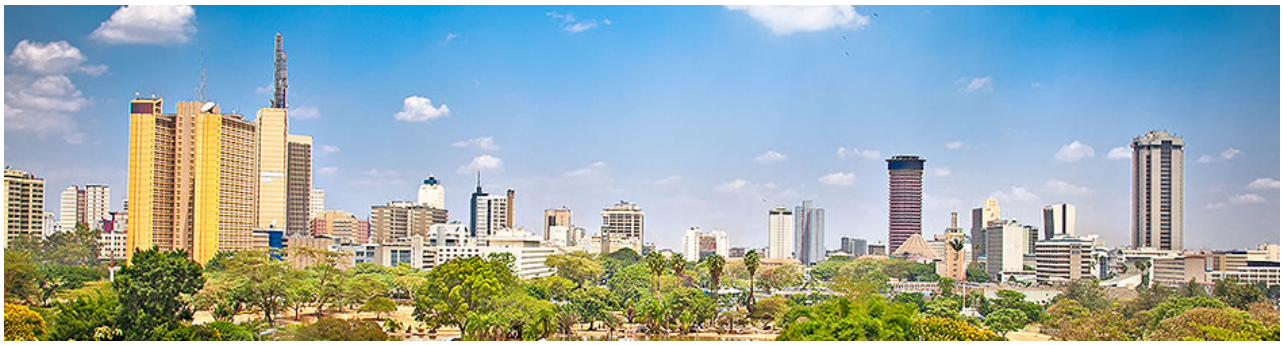
DATA PROTECTION LAWS OF THE WORLD

Kenya

DLA PIPER

KENYA



Last modified 22 January 2021

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.

DEFINITIONS

Definition of 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.

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).

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.

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.

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.

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 the data.

BREACH NOTIFICATION

Breach Notification

Section 43 of the Act

Data controllers have an obligation to notify the DPC of any breaches within 72 hours of becoming aware of a breach. On the other hand, data processors are required to inform data controllers of any breach within 48 hours of becoming aware of such a breach.

The data controller must notify the data subject of such breach without undue delay.

Under the Regulations, civil registration registries must also notify the DPC of any personal data breach. However, no timelines are stipulated for this requirement. The Regulations also grant the data subject the power to notify the relevant civil registration registry and the DPC where the data subject suspects that their personal data has been breached. This notification must be done within fourteen days of such a suspicion.

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.

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.

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 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 on-line privacy. However, this may be prescribed in the regulations or future amendments to the Act.

KEY CONTACTS

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

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

Dennis Gathara
Associate
IKM Advocates
T +254 722 898 393
dgathara@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.