CLIENT ALERT

DATA PROTECTION ACT, NO. 24 OF 2019

EXECUTIVE SUMMARY

On November 8th, 2019, the President signed into Law the Data Protection Act, 2019 ("DPA") and the same came into effect on November 25th, 2019. The Act gives effect to Article 31 (c) and (d) of the Constitution of Kenya, 2010 which guarantees the right to privacy to every citizen.

The DPA applies to natural and legal persons, public authorities, Agencies and other bodies.

Data has been classified into two: personal data and sensitive personal data.

The DPA establishes the Office of the Data Protection Commissioner ("DPC") who is to be recruited and employed by the Public Service Commissioners.

The Act introduces mandatory registration and it is an offence to act as a data processor or data controller unless duly registered with the DPC.

Data processors and data controllers are to adhere to laid down obligations among them employing security measures to prevent unauthorized access, disclosure or loss of the personal data collected by them.

Data must be processed in a manner that: upholds the data subject's right to privacy; lawfully; limited to the purpose for which it is collected; limited to the purpose for which it is collected; accurate and up to date; kept in a form which identifies the data subjects for no longer than is necessary; and not transferred outside Kenya save as permitted in the Act.

There are penalties for non-compliance with the provisions of the Act. There is a general penalty of a fine not exceeding Kenya Shillings Three Million Shillings (Ksh. 3,000,000) or imprisonment for a term not exceeding ten (10) years, or to both.

It is important to note that the Act affects operations across all sectors where personal data is handled including Media, Telecommunication, Banking and Financial sectors, Hospitality, Health, Transport, Education, Energy, Retail, Public Sector in general amongst other sectors.

It is vital to be acquainted with the provisions of the Act to ensure compliance with the laid down rules, regulations and obligations.

We have looked at the key provisions comprehensively for further insights into the Act.

FURTHER INSIGHTS

The Data Protection Act, 2019 ("the DPA") whose provisions are with effect from 25th November, 2019, was enacted to make provision for the protection of data. This is in line with Article 31 of the Constitution of Kenya, 2010 which grants the right to privacy to citizens and

specifically privacy to; information relating to their family or private affairs and privacy of their communications infringed.

In summary the Act was enacted:

-To give effect to Article 31 (c) and (d) of the Constitution

-To establish the Office of the Data Protection Commissioner

-To make provision for the regulation of the processing of personal data

-To provide for the rights of data subjects and obligations of data controllers and processors; and for other connected purposes

The DPA is enforced by the office of the Data Protection Commissioner headed by the Data Commissioner and funds are allocated to the office by the National Assembly.

The DPA governs the processing of data which is widely defined to include collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation or use, disclosure, dissemination, alignment or combination, restriction, erasure or destruction of data. Further, the Commissioner is granted power to make delegated legislation as well as issue guidelines for the enforcement of the DPA.

CLASSIFICATION OF DATA UNDER THE DPA

The DPA has classified data into two broad categories,

1. Personal Data which is any information relating to an identified or identifiable natural person, and

2. Sensitive Personal Data which means data revealing the natural person's race, health status, ethnic social origin, conscience, belief, generic data, biometric data, property details, marital status family details and the sexual orientation.

It is important to note that the DPA offers protection through the regulation of data controllers and data processors, creation of obligations, principles and rights in data and rules of exporting data from Kenya. Each of these provisions are summarized below.

CONTROL OF DATA CONTROLLERS AND PROCESSORS (PART III OF DPA)

Under Sections 18 and 19 of the DPA, it is mandatory for data controllers and processor to be registered. These entities are required to meet the threshold for registration to be set out by the Commissioner and disclose particulars set out in the DPA.

Failure to obtain such registration is an offence.

The Commissioner is granted the power to cancel or vary the certificate of registration where information leading to registration was falsified or the data controller or processor fails to comply with the requirements of the Act.

The Commissioner may also carry out periodic audits on the processes and systems of data controllers and processors. Data controllers and processors may designate a data protection officer to ensure compliance with the DPA. Such designation may be made jointly by several entities and such an officer may be in the employ of the appointing entities.

PRINCIPLES OF DATA PROTECTION

The following are set out as the principles of data protection under Section 25 of the DPA: -

a. Processing of data in accordance to the right to privacy;

b. Lawful, fair and transparent processing of data;

c. Collection of data for explicit, specified and legitimate purpose;

d. Data is adequate, relevant and limited to what is necessary for its purpose;

e. Data is accurate and where possible kept up to date;

f. The data identifies the data subjects no longer than necessary for the purpose needed;

g. Data not transferred outside Kenya unless there is proof of adequate safeguards.

RIGHTS OF DATA SUBJECTS

The rights granted under the DPA may be exercised by the data subject, a guardian or administrator where the data subject is a child or incapacitated or any other person duly authorized. Briefly, the Rights granted are:

a. To be informed of the use of the personal data;

b. Access to the personal data;

c. To object to the processing of all or part of the personal data.

d. To correction and/or deletion or erasure of false or misleading data;

e. Right to data portability;

f. Right not to be subjected to a decision based solely on automated processing, including profiling, which produces legal effects concerning or significantly affecting the data subject unless the conditions under Section 35(2) are meet;

OBLIGATIONS OF DATA CONTROLLERS AND PROCESSORS

The DPA imposes several obligations and duties on data controllers and processors. Liability attaches upon failure to perform these obligations and duties which may be summarized as follows:

(i) To collect data directly from the data subject unless the conditions for indirect collection of data are met;

(ii) To notify the data subject of required particulars under Section 29 of the DPA.

(iii) To lawfully process data;

(iv) To carry out a Data Protection Impact assessment where the processing of data is likely to result in high risk to the rights and freedoms of a data subject;

(v) To implement appropriate technical and organizational measures;

(vi) To notify, with sufficient and prescribed particulars, the Commissioner and the data subject as soon as reasonably practical of breach to personal data;

(vii) To incorporate appropriate mechanisms for age verification and consent so as to process personal data of a child;

(viii) To restrict processing of data upon the request of the data subject where the conditions listed under Section 34(1) exist;

(ix) To anonymize personal data used for commercial purposes;

THE CONCEPT OF CONSENT TO DATA PROCESSING

Data may not be processed without the consent of the data subject and it shall be the responsibility of the data controller or processor to prove that consent for a specific purpose was granted.

As regards the concept of consent the following rules are laid out under the Act:

a. Consent may be withdrawn at any time by the data subject but such withdrawal shall not affect the lawfulness of processing done before the withdrawal;

b. In determining whether consent was freely given, account shall be taken of whether, among others, performance of a contract including provision of a service, is conditional to consent to processing of personal data;

c. Processing of data relating to a child may only be done with the consent of the child's parent or guardian and in a manner advancing the child's best interests with the exceptions of a data controller or processor exclusively providing counselling or child protection services;

d. No person shall use personal data for commercial purposes unless, express consent of the data subject is obtained or the such use is authorized under any written law and data subject has been informed of such use on collection of data.

RETENTION OF DATA

Section 39 of the DPA requires retention of data only as long as reasonably necessary to satisfy the purpose for which it was collected unless the retention is:

a. Required by law;

b. Reasonably necessary for a lawful purpose;

c. Authorized or consented by the data subject; or

d. For historical, statistical, journalistic literature and art or research purposes.

Any data that has been retained beyond the retention period is to be anonymized. This provision is worded in mandatory terms in line with parliament's objective not to identify a data subject for longer than is necessary.

PROCESSING OF SENSITIVE PERSONAL DATA

The principles of processing personal data are applicable where such data is sensitive personal data. the DPA at Part V lists grounds for which sensitive personal data may be processed as follows:

a. Processing in the course of legitimate activities, with appropriate safeguards, by a foundation, an association, or any other not-for-profit body with a political, philosophical, religious or trade union aim. Such data must relate solely to the members of such bodies or persons who are in regular contact with it and such data is not disclosed outside that body without consent of the data subject;

b. Processing relates to data which is manifestly made public;

c. Processing is necessary for purposes connected to a legal claim, carrying out obligations and exercise of specific rights of a controller or data subject or protecting the vital interest of the data subject or other person legally or physically incapable of giving consent;

d. Personal data may only be processed by or under the responsibility of a health care professional or by a person subject to the obligation of professional secrecy.

TRANSFER OF PERSONAL DATA OUTSIDE KENYA

The following conditions must be met before data is transferred outside Kenya:

a. The transferor has given proof to the Commissioner that appropriate safeguards, jurisdictions with commensurate data protection laws, have been taken with respect to the security and protection of personal data;

b. The transfer is necessary for the performance or conclusion of a contract between the data subject and the Data controller or processor; matter of public interest, establishment, exercise or defence of a legal claim, protection of vital interest of the data subject or other persons incapable of giving consent, and for the legitimate interest of data controller or processors which do not override the interest and freedoms of data subjects.

c. processing of personal data out of Kenya shall only be effected upon obtaining consent of a data subject and confirmation of appropriate safeguards.

EXEMPTIONS

Section 51(1) of the DPA provides that data controllers and processors are not exempt from complying with the data protection principles. However, Section 51(2) exempts the following from the provisions of the Act:

a. processing of personal data by an individual in the course of a purely personal or household activity;

b. processing is necessary for national security or public interests;

c. disclosure is required by or under any written law or by an order of the Court.

d. Personal data processed only for research if data is processed in compliance with relevant conditions and results of research are not availed in a form that identifies the data subjects;

Additionally, Section 52 exempts the applicability of the Data protection principles to the following:

a. processing undertaken by a person for the publication of a literary or artistic material;

b. publication where the data controller reasonably believes is in public interest;

c. where in all circumstances, the data controller reasonably believes compliance with the provision is incompatible with the special purposes.

ENFORCEMENT (PART VII OF THE DPA)

The provisions of the DPA are enforced through administrative, criminal and civil means. Complaints by aggrieved persons to the Commissioner are to be determined within 90 days.

Administrative

The Commissioner may impose administrative penalties to a maximum of Five Million Shillings (5,000,000) or 1% of the undertakings previous year turn over whichever is less. Appeals from the administrative functions of the commissioner lie with the High Court.

Criminal

Offences created under the DPA carry a general penalty of a fine not exceeding Three Million Shillings (Ksh 3,000,000) or imprisonment not exceeding ten (10) years.

Some of these offences include; obstruction of investigative functions of the Commissioner and unlawful disclosure of personal data.

Civil

Damages for both financial loss and distress are recoverable by a person who suffers damage as a result of contravention of the DPA. Further, the Commissioner may seek a preservation order from the court where data is vulnerable to modification or loss.

CONCLUSION

The provisions of the DPA affect any person or entity, both public and private, that holds personal data.

Consequently, the DPA makes amendments to several existing laws to require the bodies and persons holding information collected under these Acts to adhere to the data protection provisions laid out under the DPA. Some of these Act include: Statutes relating to Education, Capital Markets Authority, Employment Act, The Kenya Information and Communications Act and the Anti-Money Laundering and Proceeds of Crime Act among others.

Please reach out to us if you require specific advice on the Data Protection Act, 2019.

(i) Benard Murunga
Partner
E: murunga@simba-advocates.com

(ii) Perpetua N. Mwangi
Partner
E: perpetua@simba-advocates.com

(iii) Reagan Etale
Associate Advocate
E: reagan@simba-advocates.com

(iv) Monica Wairagu
Associate Advocate
E: monica@simba-advocates.com

SIMBA & SIMBA ADVOCATES

6th Floor, Finance House, Loita Street

P. O. Box 10312-00100

Nairobi, Kenya

T: +254 20 2219401/ 2221933/ 2241927

+254 751603166/ 746622396

E: simba@simba-advocates.com/

info@simba-advocates.com

www.simba-advocates.com