TELECOMMUNICATIONS, MEDIA & TECHNOLOGY
Kenya

Client Alert

TRIPLEOKLAW ADVOCATES

November 2019

What the Data Protection Act No. 24 of 2019 means for your business

The Data Protection Act No. 24 of 2019 (the Act or DPA hereinafter) which was enacted on 8th November 2019 has a commencement date of **25th November 2019**. Its preamble states that it is meant to give effect to Article 31 (c) and (d) of the Constitution. These provisions guarantee that every person has the right to privacy, including not to have information relating to their family or private affairs unnecessarily required or revealed and not to have the privacy of their communications infringed.

The Act is a clean-up of several bills that were introduced previously then withdrawn for one reason or the other. TripleOKLaw, having specialized lawyers in the data protection and Privacy law was actively involved in the stakeholder process continuously giving feedback on circulated draft bills. See our most recent client alert on the data protection bill at www.tripleoklaw.com

The new law comes against the backdrop of European Union's General Data Protection Regulations (EUGDPR). Most companies operating in Kenya were still grappling with compliance. Notably, the provisions of the Act mimic those of the EUGDPR and therefore companies that had taken steps towards compliance with EUGDPR will be a step ahead.

Who is affected by the Act?

The Act limits its scope to data controllers or processors who are established and ordinarily reside in Kenya and process personal data of natural persons while in Kenya **OR** If they are not established or resident in Kenya, they process personal data of data subjects located in Kenya. This scope captures anyone

Contacts

For more information please contact:

Catherine Kariuki
Ckariuki@tripleoklaw.com

Janet Othero
jothero@tripleoklaw.com

Michael Michie
Mmichie@tripleoklaw.com

whose operations involve collection or processing of personal information pertaining to Kenyan residents. For instance, any person running an app that collects personal information is expected to comply.

Unlike the GDPR which provides a threshold for those who are subject to the act by basing it on some factors like number of employees etc, the Act is silent on this.

The overall object and purpose of the Act is to regulate and lay down the principles under which processing of personal data ought to be done. It further establishes the legal and institutional mechanisms for protection of personal data to protect the privacy of individuals.

Digital landscape in the Kenyan market

The Act is a timely legislation in this age of digital disruption where most individuals access multiple digital platforms for goods and services. This is the same for most entities that are leveraging on dynamic technological solutions to further their business strategies. Further, many businesses in Kenya leverage on data to drive their business. In the financial services and payments ecosystem, there is a lot of integration hence movement of data between the different parties.

There has been insufficient legislation on data protection in Kenya against a backdrop of robust technological innovations. The consequence was that with any digital product offering that required a user to submit their personal information, the user was left extremely unprotected should this information be used in a manner contrary to what he expected. Just like the EUGDPR and European residents, this Act seeks to primarily protect Kenyan residents.

What key provisions of the DPA should you familiarize yourself with?

Most entities (Where applicable this will also refer to natural persons processing personal information) incorporated, registered and operating in Kenya are already subject to some form of regulation or applicable statute. This Act introduces a further grouping of these entities depending on how they relate to data subjects and not what the statute refers to them.

The definitions on what one would think are common terminologies such as data or processing are extensive in light of the troves of information parties have been submitting, collecting and storing as businesses leverages on technological solutions to offer goods and services.

All affected parties must be aware of the extensive definitions of key terms in the Act including;

i. Data-*means information which-*
   a) *is processed by means of equipment operating automatically in response to instructions given for that purpose;*
   b) *is recorded with intention that it should be processed by means of such equipment;*
   c) *is recorded as part of a relevant filing system;*
   d) *forms part of an accessible record and it does not fall within a-c;*
   e) *is recorded information which is held by a public entity and does not fall within a-d above.*

ii. Data Controller-*means a natural or legal person, public authority, agency or other body which alone, or jointly with others determines the purpose and means of processing of personal data;* This extends to anyone who collects data through automated processes for a certain purpose.

iii. Data Processor- *means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller;* This covers third parties who do not directly collect the data from the subject but through their relationship with the data controller have access to such data and process it e.g financial service firms (controllers) who collect customer data (data subject) that partner with payment service providers or software solution vendors(processors).

iv. Data Subject- *means an identified or identifiable natural person who is the subject of personal data.* Other classes of legal persons like corporates etc are not protected. Further, only Kenyan residents are protected.

v. Personal Data-*means any information relating to an identified or identifiable natural person.* This covers identifiers such as names, home address, e-mail address, I.D number, location address, advertising identifiers etc.

vi. Personal data breach-*means the breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, access to, personal data transmitted, stored or otherwise processed.* This obviously has implications on existing business policies.

vii. Processing-*means any operation or sets of operations which is performed on personal data or on sets of personal data such as:-*

a) Collection, recording, organisation, structuring;
b) Storage, adaptation or alteration;
c) Retrieval, consultation or use;
d) Disclosure by transmission, dissemination or otherwise making available; or
e) Alignment or combination, restriction, erasure or destruction.

Notably, just collecting the information is regarded as processing.

When it comes to collection of personal data, the Act is alive to the fact that this can be collected indirectly, other than from the data subject. Such circumstances include from public sources, with consent from the data subject or from a source that will not prejudice the interests of the data subject.

The Act recognizes that indirect collection of personal data from other sources may be necessitated in order to prevent, detect, investigate, prosecute or punish a crime; enforce a law or protect the interests of the data subject or a person.

There are laid out principles for processing personal data. The implication of this provision is that entities will be forced to undertake a data mapping exercise to establish the amounts and classification of data they collect and store in their systems or manually. They will then need to honestly question themselves whether all this data is important and necessary for their delivery of services and goods. Most of the data may turn out to be irrelevant, unnecessary or even outdated and some even procured without the data subject's consent. The Act states the principles of personal data processing to include: -

a) Processing in accordance to right to privacy;
b) Lawful, fair and transparent processing;
c) Explicit, specific and legitimate purposes in collecting data;
d) Adequacy, relevance and limitation as to what data is necessary;

e) Collection after a valid explanation is provided;
f) Accuracy and up to date, with availability of correction without delay;
g) Kept only for timelines necessary for purpose it was collected;
h) Portability outside Kenya only upon consent or proof of adequate safeguards;

Given the general nature of these principles, it would then be up to the data controller or processor to demonstrate compliance, for instance that they have processed the personal information fairly and in a transparent manner. This is all entrenched on the business's systems and policies.

In addition to the rights guaranteed in Article 31 (c and d) of the Constitution, the data subject has a right to:-

a) Be informed of the use to which their personal data is to be put;
b) Access their personal data in custody of the data controller or processor;
c) Object to the processing of all or part of their personal data;
d) Correct false or misleading data;
e) Delete false or misleading data;
f) Data portability in a machine-readable format within reasonable time

Organizations must restructure their business processes to facilitate this in case a data subject elects to enforce any right.

Consent is Key. In collecting personal data, data controllers and processors have a duty to notify and inform the data subject on all the aspects highlighted above regarding processing of the data. Only after consent is procured from the data subject, can the data controller or processer commence with processing. The burden of proof for establishing the consent lies with the data controller or processor. There are certain exceptions to consent from a data subject provided in the Act, for instance if the processing is necessary for legal compliance, public interest or a statutory task by public authority.

The Act advises entities whose processing operations are likely to result in high risks to the rights and freedoms of a data subject to carry out a data protection impact assessment (DPIA) in consultation with the DC.

In light of advanced technologies being used by various entities to promote their business objectives the Act states that a data subject has a right not to be subjected to a decision based solely on automated processing. This also includes any instances of profiling. Many businesses leverage on A.I in their decision making. Where the consequence is to produce legal effects concerning or affecting the data subject, the data subject's rights will be infringed. There are exceptions to this provision such as where consent has been issued or where there is legal authorisation.

The Cabinet secretary has power to prescribe certain nature of processing that shall only be affected through a data server or data centre in Kenya. This would have far reaching consequences for businesses. Notably, many technology companies have been setting up data centres across Africa and enactment of this Act may inform more activity in the Kenyan Market.

Processing of Sensitive Personal Data

The Act details sensitive personal data to include 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 children's parent, spouses) sex or sexual orientation of the data subject. The Act introduces a new look at processing data on the health of a data subject.

It has now become a common occurrence for sensitive data and health data to be revealed by unauthorised persons. Government agencies are, quite concerningly, the holders of most of the sensitive data in Kenya. The sheer magnitude of it is quite impressive. This is in addition to other entities whose services revolve around collection and processing sensitive and health data such as insurance companies, hospitals and referral health service providers. How these entities inter-relate and share data or issue instructions for processing data will need to be relooked to fulfil the provisions of this Act.

Transfer of personal data outside Kenya

A data controller or processor may transfer personal data outside Kenya only where: -

a) The data controller or processor has given proof to the DC on the appropriate safeguards relating to the security and protection of the personal data;
b) Or in addition to the above, is transferring to jurisdictions with commensurate data protection laws;
c) The transfer is necessitated by contractual obligations with the data subject, public interest, legal claim or compelling legitimate interests.

When it comes to processing sensitive personal data, mandatory consent of the data subject is required.

Outsourcing data storage and processing to entities based outside Kenya will need to be assessed in light of the provisions of the Act. While most developed countries have the relevant legislation, there is need for one to satisfy themselves and the DC of the safeguards these entities have in place. This has an implication on contract negotiations and implementation especially of inspections has to be done. Further, for regulated entities like banks that already have some form of cyber security and data protection restrictions applicable to them, can they rely on CBK's approval to demonstrate compliance with the DC's office?

Exemptions

There are instances where the provisions of this Act will not apply when it comes to processing of personal data:-

a) For purely personal or household activities;
b) ***If it is necessary for national security*** or public interest;
c) Court orders or written law requires disclosure.

The principles of processing personal data shall not also apply when it comes to certain aspects of journalism, literature or arts, although this will be further subjected to a code of practice to be prepared by the DC.

When it comes to data for research, historical and statistical purposes, the data controller shall have in place safeguards and ensure that this information is not published in an identifiable form.

Enforcement

Any aggrieved data subject will have a right to lodge a complaint with the DC, after which the DC shall investigate and conclude the matter in ninety days.

The Act establishes the office of the Data Protection Commissioner (DPC hereinafter) headed by a Data Commissioner (DC hereinafter) and further designates it as a state office. The DC has the mandate to carry out investigations, facilitate alternative dispute resolution under the Act, summon witnesses and impose administrative fines for non-compliance.

The DC has authority to issue an enforcement notice to any party that refuses or is refusing to comply with the provisions of the Act. The DC can also issue a compliance notice requiring the party to comply within a period not less than 21 days. Failure to comply with an enforcement notice will upon conviction result into a fine of Kshs 5,000,000/- or two-year imprisonment or both.

An aggrieved party who suffers damage from infringement is entitled to compensation and can also sue for damages. This would give rise to civil suits and possibly class action suits against a controller or processor.

The DC in carrying out his investigative mandate, including carrying out of searches, should not be obstructed or impeded. Any failure to assist, give information or grant access to the DC will upon conviction attract a fine of Kshs 5,000,000/- or two-year imprisonment or both.

The DC may issue penalty notices for specified amounts where a party has failed or is failing to comply with provisions of the Act. The DC shall consider various factors listed in the Act in determining the amount of the penalty.

The maximum penalty that the DC can impose under this Act is upto Kshs 5,000,000/- or 1% of an undertaking's annual turnover of the preceding financial year.

Notably, the DC has the power of entry and search in a premise in relation to discharging it's functions. Controllers or Processors who are in contravention should expect to encounter dawn-raids.

What does the DPA mean for your business?

The provisions of the Act certainly cut across all businesses in Kenya. It also means that all functions of a business are affected e.g Human Resources, sales, operations etc. Due to the far-reaching implications, compliance should be board-led.

For regulated entities, this Act introduces yet another aspect of oversight, together with inspections and routine assessments, through the DCs office. Entities will need to relook their costs and resources on regulatory compliance.

Registration with the office of the DC is mandatory for entities that are classified as either as data controllers or processers. A self-assessment is required.

Client Alert

In light of the diverse sectors most data controllers and processors operate in, the DC will issue varying requirements. Entities need to be alive to the nature of their operations and their relationship with data subject and anticipate the obligations the DC may impose on them. This Act may not be necessarily a one size fits all and as such customization is recommended.

When it comes to requirements needed for registration, parties will need to have certain policies such as data protection and privacy, cybersecurity and contractual indemnifications that may be submitted to the DC to expedite registration. The result of being issued with a registration certificate is that an entity achieves another mark of compliance that not only endears it to data subjects but other business partners who can rely on this as a quality assurance.

Of further importance is the creation of the position of the Data Protection Officer. The DPO is the face of an organisation on all matters data protection and as such they need to be easily accessible. They also act as the liaison to the DC's office. Ideally, a staff member with the requisite skill may be seconded to be the officer or may be separately recruited to fill the position. Groups of companies can appoint one officer to serve all the companies while public bodies within certain organisational structures can appoint one officer.

The cost implication of compliance cannot be overlooked. While the EUGDPR gave entities a two-year moratorium to achieve minimum compliance, this Act is relatively silent on a moratorium. The fact that this is a rather technical procedure, that is not similar across board, should advise the DC to issue piecemeal regulations that is sector customized. We expect to see the Data Commissioner, when appointed, issue further guidelines and codes of practice on some of the grey areas which, if implemented as is, may lead to unintended consequences. However, with such a technical and large process required to be compliant, organisations should start immediately as the provisions inform a lot of in-house changes ranging from new policies and systems, changes in cyber security and data protection measures, internal training and awareness and necessary appointments.

In conclusion, all entities operating in Kenya ought to look at their business models to determine how they can best categorise their relationship with data subjects and/or with other parties.