Regulatory Alert

Implications of the GDPR on Kenyan entities

June 2018

Introduction

On 25th May 2018, the General Data Protection Regulation ("GDPR") came into force in European Union (EU) member states, revolutionizing the way that personal data is collected, handled, transferred and destroyed. Controllers and Processors (as defined below) of Personal Data need to adhere to the GDPR and Data Subjects (as defined below) need to understand their fundamental human right to data privacy.

The GDPR, by virtue of its territoriality provisions, is automatically enforceable in EU member states. The processing of any information of any individual located in the EU is covered by the GDPR, regardless of where the processing occurs. Each EU State is required to appoint a Supervisory Authority to monitor the application of the GDPR.

For countries such as Kenya, which does not have any comprehensive data safety laws in place, there are legitimate concerns over how the GDPR applies, who is protected and the obligations on Data Controllers and Processors, especially in light of the high penalties in the GDPR for non-compliance, which can go up to twenty million Euro (EUR 20 000 000) or four percent (4%) of the total worldwide annual turnover of a company.

This article will address some of the key provisions of the GDPR as they apply to Kenya.

The current legal status of Data Protection in Kenya

The right to privacy is enshrined in the Constitution of Kenya (2010). In particular, data protection is recognized in Article 31(c) and (d) of the Constitution, which provide that every person has a right to privacy, which includes the right not to have:

c) information relating to their family or private affairs unnecessarily required or revealed; or

d) the privacy of their communications infringed.

Various sector laws and regulations also contain provisions requiring relevant regulated entities to put in place mechanisms for maintaining client confidentiality and data protection and security. Examples of these include legislation and regulatory guidelines governing the banking, telecommunications, capital markets and insurance sector.

Kenya does not, however, have a stand-alone comprehensive law governing data protection. A draft Data Protection Bill was published several years ago, but has yet to be enacted. Additionally, Kenya is a signatory to the African Union Convention on Cyber Security and Personal Data Protection, but this Convention is not enforceable without being adopted via local legislation. We expect that comprehensive data protection legislation, modelled on the EU's GDPR, will be passed later in 2018.

Definitions

The GDPR contains the following important definitions that are central to understanding its application:

- **Personal Data** is any information relating to a person that can be used to directly or indirectly identify them. This includes full names, an identification number, location data and an online identifier. It also includes data on factors specific to the person that can be used to identify them such as physical, physiological, genetic, mental, economic, cultural or social identity data.
- **A Data Controller** is a natural or legal person that determines the purposes and the means of processing Personal Data.
- **A Data Processor** is a natural or legal person that carries out any manual or automated operation on Personal Data such as collecting, recording, organizing, storing, altering, retrieving, disclosing, disseminating, combining, erasing or destructing.
- **A Data Subject** is any person located in the EU.

Who is protected?

The Personal Data of all persons located in the EU (Data Subjects) is protected by the GDPR.

Who has obligations?

Both Data Controllers and Data Processors have obligations under the GDPR if they deal with the

pwc

Personal Data of Data Subjects for the purposes of:

a) the offering of goods or services to Data Subjects (irrespective of whether a payment is required); or

b) the monitoring of the behavior of Data Subjects (such as using cookies).

Does the GDPR apply to Controllers and Processors in Kenya?

The GDPR will apply to Data Collectors and Processors in Kenya that:

- Collect and Process the Personal Data of Data Subjects. These include (but are not limited to) the following: banks, tour agencies, hotels, multinational companies, marketing agencies, hospitals and landlords;
- Have employees that are Data Subjects;
- Offer goods and services in the EU. The net of what constitute goods and services has been cast very wide. A Kenyan company with an online presence offering goods and services to EU citizens will be bound even if the company has no presence in the UK;
- Have a partnership with an EU business where Personal Data is shared. The GDPR puts an onus on EU businesses to ensure their third-party suppliers handling Personal Data are compliant. This could impact multinational organizations with a presence in Kenya that are used to sharing data across borders.

General Principles relating to Personal Data

Chapter II of the GDPR sets out six principles relating to the controlling and processing of Personal Data of Data Subjects. Personal Data must be:

Lawfulness and Transparency Processed lawfully, fairly and in a transparent manner	**Purpose Limitation** Collected for a specified, explicit and legitimate purpose
Data Minimization Adequate, relevant and limited to what is necessary for processing purposes	**Accuracy** Accurate and kept up to date
Storage Limitation Kept in a form which does not permit identification of Data Subjects for longer than is necessary	**Integrity and Confidentiality** Processed in a manner that ensures appropriate security

Obligations of Data Controllers

Data Controllers are required to:

1. Collect consent from Data Subjects to having their Personal Data collected. Consent must be freely given, specific, informed and unambiguous.
2. Implement appropriate technical and organizational measures to ensure they are collecting, processing and disposing of Personal Data in accordance with the principles of the GDPR;
3. Put in place technical measures to safeguard Personal Data throughout the period of control;
4. Only transfer Personal Data to a country or organization that is GDPR compliant;
5. Only use a Data Processor that is GDPR compliant;
6. In the event of joint processing/controlling, all Data Controllers will have to ensure there is a contract in place setting out each party's responsibilities for GDPR compliance;
7. Inform the relevant supervisory authority in the case of any breach within seventy two (72) hours of becoming aware of the breach;
8. Develop mechanisms to communicate with Data Subjects on their Personal Data in their control. This includes total transparency with regard to how data is being used and the processing purpose.

Specific obligations of Data Processors

Data Processors are required to:

1. Carry out a data protection impact assessment when implementing new technologies and ensure that all technology in place is of the latest standards;
2. Take steps to minimize data risk by using encryption, pseudonymization and regular security testing;
3. Only process data upon written instruction from a Data Controller and upon confirmation that the Personal Data has been collected with the consent of the Data Subject;
4. Only process data for purposes entrusted to them by the Data Controller;
5. Keep a record of all processing operations carried out on Personal Data and build a data inventory;
6. Inform Data Controllers of any breach within seventy two (72) hours of becoming aware of the breach;
7. Upon request from the Data Subject or the Controller, delete all Personal Data from their systems.

Rights of Data Subjects

Chapter III of the GDPR sets out all the rights of Data Subjects

Right to Consent

If data is being collected, consent must be given in a specific and informed manner. The Data Subject has the right to withdraw consent at any time (although this will not impact the lawfulness of the processing done prior to withdrawal).

Right to receive a notification on breach

In the event of a data breach, Data Controllers are required to report to the relevant local supervisory authority within seventy two (72) hours of becoming aware of the breach. If the breach poses a high risk to the Data Subject, the Data Subject must also be notified without undue delay. It is not clear what will occur when data breaches occur in countries without a local supervisory authority but it is expected that an EU supervisory authority will liaise with overseas regulators to monitor breaches. We anticipate that the impending Kenyan data protection legislation will establish a relevant authority to enforce compliance.

Right of access

Data Subjects are able to ask whether their personal data is being processed. A Data Controller must then provide a copy of the Personal Data held free of charge in a prescribed format within one month of receipt of the request. This should outline:

a) The type of data being processed;

b) The recipients of the data;

c) The period of time the data will be processed; and

d) Meaningful information about how the information is used to profile and the logic behind the processing.

Right to be informed

Where Personal Data is being transferred to another country or organization, the Data Subject has the right to be informed of the appropriate safeguards relating to the transfer.

Right to be forgotten

Data Subjects have the right to request the erasure of all their Personal Data. However, this is not an absolute right and applies only in the following circumstances:

a) If the Personal Data is no longer necessary for the purpose it was originally collected;

b) If the Data Controller was relying on consent as the lawful basis for holding data and the consent is withdrawn;

c) If there is no overriding legitimate interest to continue the processing;

d) If the Personal Data is being processed for marketing purposes and the Data Subject objects; or

e) If the Personal Data was being processed unlawfully.

Data Portability

A Data Subject can request their information in a commonly used and machine readable format to be submitted to another Data Controller free of charge.

Data Protection Officers

All Data Controllers and Processors should appoint a Data Processing Officer and an EU representative if:

a) the core activities of the Data Controller of Processor consist of processing Personal Data of Data Subjects on a large scale;

b) the core activities of the Data Controller of Processor consist of processing special categories of Personal Data of Data Subjects (special categories of personal data includes data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, health or sexual orientation);

c) where there is a potential that rights and freedoms of Data Subjects are at risk.

A Data Processing Officer will be tasked with overall GDPR compliance to ensure appropriate data protection strategies are in place.

An EU representative should act on behalf of the Controller or the Processor within the EU and may be addressed by any supervisory authority.

Questions to ask yourself as a Kenyan company

The GDPR is not a one-size-fits all regulation and it is important for organizations to understand their operations, services and the extent to which they need to comply. To this end, companies need to understand the following aspects before any GDPR compliance can be undertaken:

1. Do you control or process the information of any persons that qualify as Data Subjects? (When carrying our client due diligences, companies should ask whether the client is resident in the EU and request they receive a notification in the event the client relocates to the EU).
2. Does your core business consist of data processing and to what extent does that involve the processing of Personal Data of Data Subjects?
3. How is Personal Data treated and secured?
4. Is all the Personal Data collected limited to what is necessary for the core function of the business? Can any unnecessary data be deleted?
5. Are there any agreements with other parties for the sharing/ outsourcing of Personal Data and are these GDPR compliant?
6. Are any contracts in place with Data Subjects and are these GDPR compliant?
7. How can systems to re-designed to enable Personal Data to be protected end to end?
8. What rights of access to Personal Data do Data Subjects have?
9. Do you have the ability to implement the following measures?
   a) *pseudonymisation and encryption of personal data;*
   b) *confidentiality and integrity of processing systems; and*
   c) *regular testing and evaluation of such measures.*

Offences and Penalties

These are set out in Chapter VIII of the GDPR

Is it yet to be seen how fines will be enforced on non EU entities without any assets within the EU. It is likely that EU Supervisory authorities will liaise with local regulatory authorities to enforce lack of GDPR compliance.

Nonetheless, the reputational damage and loss of customer trust are key considerations for non EU companies to comply with the GDPR.

10 000 000 EUR, or up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher	• Failing to obtain adequate consent when collecting Personal Data of children • Collecting Personal Data that is unnecessary for the purpose of processing • Failing to implement "Data by Design" principles • Failing to allocate responsibilities between joint Data Controllers • Failing to appoint a representative in the EU if needed • Failing to appoint a data protection officer if required. • Failing to keep records of processing activities • Failing to comply with the instructions of a supervisory authority • Failing to provide a supervisory authority with a breach notification • Failing to provide a Data Subject with a breach notification when required • Failing to carry out an impact assessment for new technology • Failing to appoint a data protection officer if required
20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher	• Failing to abide by the basic principles for processing, including conditions for consent • Transferring Personal Data to a third country or an international organization without adequate GDPR compliance • Failing to abide by an order from a supervisory authority

The GDPR and contracts

In light of the high penalties in the GDPR, Kenyan companies that are in contractual relationships with EU Data Controllers or Processors may come under pressure to enter into Data Processing Agreements to provide warranties and indemnities regarding GDPR compliance.

They may also be subject to more stringent information disclosure provisions in the Data Processing Agreements, designed to give assurance to the EU entities that the GDPR risk is being mitigated.

Therefore, even if there is doubt regarding the applicability of the EU law to non- EU entities, Kenyan companies could still be drawn into the GDPR net through contractual obligations.

Please get in touch with the PwC Kenya offices should you need any assistance in drafting or reviewing contracts to ensure GDPR compliance and to ensure a clear understanding of the implications of such contracts.

Way forward

The GDPR compliance journey will be complicated for many organizations and it is recommended that significant time and resources be invested to ensure full compliance.

For more information please contact any of the contacts below.

Joseph Githaiga
Head of Regulatory Compliance & Advisory
joseph.githaiga@pwc.com
+254 20 285 5401

Gachini Macharia
Manager
gachini.macharia@pwc.com
+254 20 285 5805

Jehaan Ara Kassam
Senior Associate
jehaan.kassam@pwc.com
+254 20 285 5026