# Review of the General Data Protection Regulation and Understanding the Extraterritorial Reach

August 2018

## Executive Summary

- To determine if the GDPR extraterritorial reach applies, a Kenyan entity would have to consider if it offers goods or services to EU residents. However, if the data processing the foreign entity undertakes is only occasional data processing then this requirement is negated.
- If it applies, the Kenyan entity may need to appoint a data representative based in the EU to deal with queries and complaints.
- Even if the GDPR does not apply it may be that EU entities may still ask a Kenyan entity to put in place various safeguards.

## Background

The General Data Protection Regulation (**GDPR**) came into effect on 25 May across all EU countries. It is a unifying regulation and therefore applies to the whole of the EU without requiring the each EU country to pass enabling legislation.

The GDPR regulates the use of personal data of EU residents with the objective of protecting the right to privacy. It is important to note that the GDPR applies a residency test and not a citizenship test to determine if an individual can be protected by the regulation. Therefore, for example, a Nigerian national living in Brussels can rely on the GDPR.

In this note we look at some of the practical issues around the new regulation.

## What is considered personal data?

The GDPR considers any information relating to an identified or identifiable individual, either directly or indirectly to be personal data. This could be as simple as a name or a number or could include other identifiers such as an IP address or a cookie identifier, or other factors.

## Who is regulated?

There are two categories of data handlers who are regulated:

(a) **Data controllers**. These are individuals or legal entities that determine the purposes, conditions and means of processing personal data;[1] and

(b) **Data processors**. These are either individuals or legal entities that process personal data on behalf of a controller.[2]

[1] Article 4 (7)
[2] Article 4 (8)

**Who is not regulated?**

Natural persons carrying out purely personal or household activities and authorities dealing with criminal investigations, prosecution etc are exempt from the requirements of the GDPR. [3]

**What are the responsibilities of a controller?**

The controller is responsible for implementing the operational measures and policies to ensure that personal data is being handled in accordance with the Regulations.[4] Key to this is the data controller's responsibility to demonstrate that the data subject has consented to their personal data being processed.[5] In relation to the consent required the GDPR stipulates that:

(a) When the data subject is giving a written consent and the consent includes other matters, the consent for the use of personal data needs to be presented in such a manner which clearly distinguishes it from the other matters.

(b) The consent needs to be intelligible and use plain language.

(c) The consent needs to be freely given. In determining whether consent has been freely given it will take into account whether the provision of the service is conditional on agreeing to the processing personal data that is not necessary for the performance of the contract / service.

(d) The data subject has the right to withdraw their consent at anytime and this should be easy to do.

The GDPR prohibits the processing of personal data revealing racial or ethnic, political, religious or philosophical opinions or, union membership, genetic or biometric data, data concerning health, sec life or sexual orientation is prohibited unless the data subject has given explicit consent, or the information is required for the compliance of a specific law etc.[6]

**Can a foreign company / person be subject to these regulations?**

Yes, a foreign company can be subject to the GDPR if they are either a controller or processor who offers goods or services (not necessarily paid) to EU residents or monitors the behaviour of EU residents. To determine whether an entity 'offers goods or services' the recitals of the GDPR clarify that what will be looked at is the intention of the processor or controller. For example simply having a website that an EU resident can access is not sufficient to meeting this test.[7]

To understand the intention of the processor or the controller the recitals state that other factors like the option to interact with the website in the EU national native's language; use of the EU currency; or using EU residents' testimonials as a means of marketing services / goods to other EU residents can be used to

[3] Article 2
[4] Article 24
[5] Article 7 (1)
[6] Article 9
[7] Recital 23

determine the controller or processors intention.[8] Unfortunately, this is a subjective test that will require a case by case analysis.

The Court of Justice of the European Union has, through various decisions, given further guidance on the factors that would be considered to determine if goods or services were being offered. This includes looking at whether there was any payment of money to a search engine to facilitate access by those within an EU Member State; or considering the "international nature" of the relevant activity (e.g. certain tourist activities) including the use of telephone numbers with an international code.

**Steps to take if the GDPR applies**

Companies are advised to first undertake a data audit to understand:

(a) what data they process;

(b) for what purposes; and

(c) who they share the data with.

Once this exercise is complete companies can then begin to formulate appropriate policies to comply with the rules. While the GDPR does not contain any hard or fast compliance rules it simply lists seven principles[9] which data processors / controllers need adhere to. These principles are detailed below. In addition member States will publish their own code of conduct which can be used as a guide in creating appropriate policies bearing in mind the size of the entity and its sector.[10]

The GDPR provides that if the controller or processor is undertaking significant data processing and are not based in the EU then they will need to appoint a representative in the EU who will act as the point of contact for any data queries and to ensure compliance with the GDPR.[11]

**Application of GDPR to a Kenyan entity that is not caught by the legislation but receives personal data from an EU entity**

The GDPR provides that if an EU company sending personal data to a third country it will need to be either on the basis of:

(a) an adequacy decision (i.e. the European Commission has determined that the country has in place adequate levels of protection for personal data);[12] or

(b) the receiving entity demonstrating that it has appropriate safeguards e.g. through contractual clauses and having in place binding corporate rules.[13] In addition the receiver will need to show that effective legal remedies are available.

[8] Recital 24
[9] Article 5

[10] Article 40
[11] Article 27
1. Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union. 2. The obligation laid down in paragraph 1 of this Article shall not apply to: a) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing;

[12] Article 45
[13] Article 46

In absence of both the data subject will either need to give explicit consent having been informed of the risks. Alternatively, if the transfer is necessary for the performance or conclusion of a contract between the data subject and the controller (or the implementation of pre-contractual measures) then the transfer of data is permitted.[14]

**Data Processing & Storage Guidance**

The GDPR provides for seven key principles that need to be adhered to, that is:

(a) **Fairness & Transparency -** data needs to be processed lawfully, fairly and in a transparent manner in relation to the data subject.

(b) **Purpose Limitation** - data is to be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

(c) **Data Minimisation** - Processing of data will be limited to what is necessary, relevant and adequate in relation to the purposes for which it is being processed.

(d) **Accuracy / the Right to be Forgotten -** Data processed should be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

(e) **Storage Limitation -** personal data is to be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods it will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

(f) **Integrity and Confidentiality** - Personal data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

(g) **Accountability -** The controller shall be responsible for, and be able to demonstrate compliance with, the above principles.

**Regulator / Enforcer and Consequences of Infringement**

The European Union has established a European Data Protection Board[15] to oversee the application of the GDPR. In addition each EU member state will appoint its own public authority (termed 'Supervisory Authority') to monitor the application of the GDPR. The Supervisory Authority can among other things:

(a) conduct data protection audits;

(b) review certifications (the GDPR creates a voluntary data protection certification mechanisms, for the purpose of

[14] Article 49

[15] Article 68

demonstrating compliance with the GDPR) ;

(c) issue warnings if it believes a GDPR violation may occur;

(d) order a processor or controller to comply with GDPR;

(e) order the controller to communicate a personal data breach to the data subject;

(f) impose limitations, and even bans, on processing;

(g) impose administrative fines;

(h) suspend data flows to a recipient in a third country or international organization; and

(i) receive complaints from data subjects.

The financial penalty to be applied will be determined by the article infringed. The GDPR provides for certain infringements a lower level limit up to €10 million, or 2% of the worldwide annual revenue whichever is higher and an upper level - up to €20 million, or 4% of the worldwide annual revenue whichever is higher. However, the Supervisory Authority can take into account: the nature of the infringement, the intention of the party, actions taken to mitigate the damage, preventative measures that were in place, history of past relevant infringements, level of cooperation the party has shown, the type of data, whether notification of the infringement was proactively reported, certification and any other aggravating or mitigating factors.

**Examples**

| Scenario | GDPR Applies? |
|---|---|
| A Kenyan tourism company is using cookies to track past customers (including EU customers) browsing history, in order to offer specific holiday packages to them. | ✓ |
| An online Maasai market goods provider in Kenya has a website that is accessible to individuals in the EU in English. The currency is KES. | X |
| A Kenyan British system school advertises for UK qualified teachers on a third party UK website. | ✓ |

For further advice about any of the information contained here please feel free to contact:

**Mahesh Acharya**
**Partner**
MAcharya@kapstrat.com