KTA
ADVOCATES & SOLICITORS

TMT

TECHNOLOGY MEDIA & TELECOMMUNICATION

NEWS ALERT

CROSS BORDER TRANSFER OF DATA & ITS LIMITATIONS

The European Union has approved the General Data Protection Regulation (GDPR) that come into force on May 25th, 2018. The Regulation lays down rules relating to the protection of natural persons with regard to the
processing and movement of personal data. Article 4 of the GDPR, defines 'personal data' as any information relating to an identified or identifiable natural person referred to as a data subject.

An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Through the GDPR, the EU has joined USA & India, among others, in affirming the right to privacy and protection of personal data as a fundamental human right. In 2017, the Supreme Court of India in

Justice K.S. Puttaswamy (Retd.) & Anor. v Union of India & Ors, WP (Civil) 492 of 2012, declared that privacy is a fundamental right protected under the country's constitution for each of its over 1.3 billion citizens.

Ironically, the regulation also give a carte blanche to EU governments, to process personal data of its citizens if it is in the interest of national security.
For companies operating in the digital space, Articles 3 & 46 of the GDPR are important as they provide for the cross-border transfer of data. Article 3, extends the scope of the GDPR to cover data processed outside the EU, as long as the data relates to a data subject who is a citizen of any of the EU countries. Consequently, the GDPR's reach, extends to EU companies that do business in Uganda.

To put this into context, banks like Standard Chartered or Barclays, that have their head offices in the UK, but offer cross border digital banking services, will have to adopt stricter procedures to comply with the GDPR in
protecting the personal data of their EU customers, that may utilize online banking services in Uganda.
Article 46, provides that any transfer of personal data to a third country can only take place if certain conditions are met by the data exporter and the data importer. If a company is transferring personal data outside of the EU, that company must identify a valid transfer mechanism to legally transfer that personal data.

The main implication of the latter, is that banks and other EU based companies must have a legitimate basis for transferring personal data to a jurisdiction like Uganda, that is not recognized as having adequate data protection regulation.

This applies to personal data that is transferred deliberately or by inadvertence in the company's ordinary course of business.
In the absence of adequate regulation, the GDPR only permits data transfers to countries without data protection regulation, if the data controller and processor gets express consent from the data subject to transfer the subjects data. Requests for consent in this case, would be separate from other terms, and must be in clear and plain language.
Another exception provided for in the GDPR, is if the EU based company uses EUapproved safeguards. The most widely used transfer mechanisms are binding corporate rules (BCRs) and model contractual clauses.
BCRs are internal data collection, retention and destruction policies adopted by multinational companies to allow transfers between different branches of the organizations.

contractual clauses are legal terms contained in a template data processing agreement, drafted and ratified by the EU. Model contractual clauses can be burdensome because companies are required to enter new model
contractual clauses to cover each new third party and each new purpose for processing or transfer.
Failure to comply in the manner above, may lead to fines of up to 4% of a noncompliant company's annual worldwide turnover and an additional EUR 20M (Twenty Million Euros) or more.
The risk is real for all EU based companies that choose to do business in an unregulated data market like Uganda.

The GDPR also applies to non EU based companies that offer goods or services to individuals in the EU and/or that monitor or track the online behavior or activities of those individuals in the EU. Local digital lenders, money transfer platforms like M-Pesa, payment platforms like Payway & other e-commerce businesses that serve clients in the EU have to comply with the GDPR or risk being fined and/or banned from offering their services to EU customers.

WHAT ORGANIZATIONS OFFERING E-COMMERCE & DIGITAL FINANCIAL SERVICES MUST DO TO COMPLY

Firstly, data controllers must put in place adequate EU sanctioned data collection, retention and destruction policies. Collection of data from subjects, must also be done in a transparent and lawful manner. In regards to consent, companies must put in place mechanisms that make it easy for subjects to request for their data to be forgotten (deleted). The right to be forgotten, was first introduced by the European Court of Justice (ECJ) in a case involving Google Spain, where the ECJ affirmed that data subjects have a "right to be forgotten" and held that Google must delete "inadequate, irrelevant or no longer relevant" data from its results when a member of the public requests it.

Companies must also hire Data Protection officers and put in place data breach notification procedures. For EU based companies, any data breach that happens in Uganda, must be reported, where feasible within 72 hours to the Data Protection Agency in the Company's home country.
Most importantly, companies should always have adequate privacy and data protection policies. For group companies, adopting binding corporate rules to facilitate intra-group transfers of data will promote compliance.
On the government side, lawmakers can no longer afford to bury their heads in the sand as failure to pass the Data Protection and Privacy Bill, may cost Uganda much needed Foreign Direct Investments (FDIs) from EU based companies that may find it too expensive (or rigorous) to comply with the GDPR if they are to do business in Uganda.

By Kenneth Muhangi

THE TEAM OF PARTNERS

JUSTUS KARUHANGA
PARTNER
Commercial & Corporate. Public, Private Partnerships (PPPs)
+256 776 000 711
jk@ktaadvocates.com

EDGAR TABARO
PARTNER
Construction Law. Commercial. Corporate
+256 752 535 390
emt@ktaadvocates.com

EDWIN TABARO
MANAGING PARTNER
Intellectual Property. Commercial Litigation
+256 754 957 977
et@ktaadvocates.com

KENNETH MUHANGI
PARTNER
Technology. Media. Telecommunications. Intellectual Property
+256 793 995 082
mk@ktaadvocates.com

URBRA House
Floor 2, Wing A, Plot 1
Clement Hill Road
P.O. Box 37366 Kampala, Uganda
Tel: 0414 530 114
Fax: 0414 531 078
Email: partners@ktaadvocates.com

Uganda • Kenya • Tanzania • Rwanda • Burundi • South Sudan
KTA Advocates & Solicitors is affiliated to the Amani IP Network

AMANI IP NETWORK

INNOVATE. GROW. DISCOVER

www.ktaadvocates.com