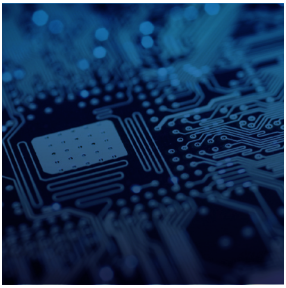
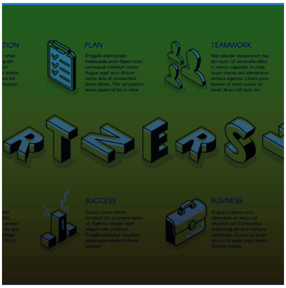
KTA
ADVOCATES
Formerly Karuhanga Tabaro & Associates

Overview of **Data Protection Regime in Uganda**

By Kenneth Muhangi

le buzz
Interview with Fashion and Lifestyle Blogger Marina the Moss





While Privacy/data protection is not always directly mentioned as a separate right in constitutions, nearly all States recognize its value as a matter of constitutional significance. Although this right is enshrined in Article 27 of the constitution, the applicability/and enforceability of the right has until recently, been a laughable notion in Uganda.

Data is information that is processed by means of equipment operating automatically & in response to instructions given for that purpose[1]. Entities dealing in data this side of the Equator, have since the dawn of (e)commerce been self-regulating and picking cues from more data protection savvy jurisdictions. That is until the new Data Protection & Privacy Act, 2019, a sui generis legislation that regulates every aspect of data collection and processing.

In the developed world, the first steps taken towards regulating data protection were taken through the council of Europe convention 1981[2]. The convention was followed by Directive 95/46/EEC[3], that required-through article three, all EU member states to protect the fundamental rights and freedoms of natural persons and in particular the right to privacy with respect to the processing of personal data.

Most recently, the European Union 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.

In Africa, the African Union (AU), recognizing the need to regulate data protection, in 2014 introduced the Convention on Cyber Security and Personal Data Protection. Expectedly however, only a handful of AU member states have assented to the convention or enacted local data protection regulation, leaving Uganda as one of only a few elite African nations to regulate data protection.

The new 2019 law, mirrors the UK Data Protection Act 1998[4] but is nonetheless groundbreaking in its own right,

[1] Data Protection Act, 2019, Interpretation section
[2] convention 108 for the protection of individuals with regard to the automatic processing of tracts
[3] OJ L 281, 23.11.1995, p.31
[4] The Data Protection Act 1998,Came into force on 1st March 2000

Overview of the Data Protection & Privacy Act, 2019

The 2019 act just like the UK Data Protection act, the GDPR & the African Union Convention on Cyber Security and Personal Data Protection, revolves around several principles concerning data protection and these are the gist of this act. They propose that a data controller/processor should be accountable to the data subject for data collected, processed, held or used; data should be collected in a lawful and fair manner; it should be adequate, minimal and not excessive, accurate, not misleading & up to-date, collected transparently, shouldn't be kept longer than necessary, should be secure and overall should only be used for the purpose for which It is collected.
The Act establishes a personal data protection office responsible for ensuring that the principles are observed.

What is Personal Data

The 2019 act, follows Article 4 of the GDPR, in defining 'personal data' as any information relating to an identified or identifiable person referred to as a data subject.

An identifiable 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, academic, genetic, mental, economic, cultural or social identity of that natural person.

The definition, seems to cover both living and deceased persons and as long as any data collected relates to that person then that data is subject to the law.
Under part (e) of the Interpretation section (Section 2), the scope of personal data is widened to include all other information which is in the possession of a data controller and includes an expression of opinion about the individual.

This may include medical records, bank account details, mobile money account details, email address, any identification number (driver's license, passport number, NIN number etc) and even an Internet Protocol (IP) address. On 19 October 2016, the Court of Justice of the European Union (the "CJEU") published its judgment in Case 582/14 – Patrick Breyer v Germany[5], in which it held that IP addresses are personal data in certain circumstances.

Specifically, the court ruled that dynamic IP addresses may constitute 'personal data' even where only a third party (in this case an internet service provider) has the additional data necessary to identify the individual – but only under certain circumstances: The possibility to combine the data with this additional data must constitute a "means likely reasonably to be used to identify" the individual.

DURANT V FINANCIAL SERVICES AUTHORITY[6] sums up personal data as data that relates to an individual if it is information that affects a person's privacy, whether in his personal or family life, business or professional capacity.

Personal data, is for all intent and purpose confidential information that cannot be shared without the express consent of the data subject[7]. In fact, Sections 17 & 18 of the Uganda Computer Misuse Act, 2011 and section 35 of the 2019 act, criminalize the unauthorized release/disclosure of such data. The aforementioned sections, are reinforced by Article 17 of the International Covenant on Civil and Political Rights (ICCP) that provides that, "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation".

Article 17 is encapsulated in Article 27 (2) of the Constitution that provides that, "No person shall be subjected to interference with the privacy of that person's home, correspondence, communication or other property."

And finally section 10 of the 2019 act that prohibits collection or processing of personal data in a manner that infringes on the privacy of a data subject.

[5] http://curia.europa.eu/jcms/upload/docs/application/pdf/2016-10/cp160112en.pdf
[6] Michael John Durant v Financial Services Authority [2003] EWCA Civ 1746, Court of Appeal (Civil Division) decision of Lord Justices Auld, Mummery and Buxton dated 8thDecember 2003.
[7] Section 22sof the 2019 act.

The Law also explains who a data subject, data processor and data controller is. A data subject is defined by the act to mean an individual from whom or in respect of whom personal information has been requested, collected, collated, processed or stored.

Sections 24-27 of the act, in compliance with the African Union Convention on Cyber Security and Personal Data Protection (AUCCSP-DP), provide for the rights of a data subject. Some of these rights include, the right to know if a data controller holds any personal data on the subject, the right to prevent processing of personal data if that processing is likely to cause unwarranted damage or distress to the subject & the right to prevent processing of personal data for direct marketing.

A data processor in relation to personal data, is defined as a person other than an employee of the data controller who processes data on behalf of the data controller. Processing means any operation which is performed on collected data by automated means or otherwise including, organizing, adapting, alternation, retrieval, erasure, alignment, combination or destruction of the data.

A data controller is defined to mean a person who either alone or jointly or in common with other persons determines the purposes for which and the manner in which any personal data is, or is to be, processed. This definition impliedly includes employees of the data controller.

Section 9 of the 2019, act prohibits the collection and processing of data that relates to religious, philosophical, political opinion, sexual, financial, health status or medical records of an individual. The exceptions being if the data is collected or processed by Uganda Bureau of Statistics, collection mandated by law on an employer, information given freely and with the consent of the data subject and collected in furtherance of the legitimate activities of a body or association.
Such associations may include religious organizations, political parties or trade unions.

Consequently, some data analytics companies like Cambridge Analytica that profile data subjects for profit may not be able operate legally in Uganda.

The now defunct, Cambridge Analytica (CA) came under fire in 2018 for the unauthorized use of data that it used to influence elections around the world.

In Kenya, CA, is accused of manipulating Kenyan voters by curating videos that exploited their fears. The videos warned social media users that a victory by opposition leader Raila Odinga would lead to disease, starvation and terrorism.

In Nigeria, a UK newspaper, The Guardian reported that Israeli hackers provided Cambridge Analytica with President Muhammad Buhari's personal emails. The e-mails that included information about Buhari’s ill health and medical records, were leaked in order to dissuade voters and to weaken Buhari’s campaign.

And most famously, CA is credited for using its algorithms to influence the US election allowing Trump to become president.

In regards to sharing data, a data controller/processor may only share data of a data subject if it is public record, the data subject has deliberately made the data public, the data subject has consented, if data is anonymized or if it is in furtherance of a law, public interest or national security [8].

Under Section 13, a data controller/processor is also mandated to inform the subject about;
a) the nature and category of work collected;
b) name and address of data collector;
c) purpose for which the data is required;
d) whether or not the supply of data is discretionary or mandatory;
e) consequence of failure to provide the data;
f) what law necessitates the collection of the data;
g) the recipients of the data;
h) existence of the right of data subject to access data, rectify and delete it;
i) period of retention of the data.

[8] Section 11 of the 2019 act.

Consent

In relation to the aforementioned personas, processing personal data is generally prohibited, unless it is expressly allowed by law, or the data subject has consented to the processing.[9]

Section 7 however provides other legal bases for collection and processing of personal data. The others are: where the collection is;

a) necessary for the proper performance of a public duty by a public body;
b) for national security
c) for the prevention, detection, investigation, prosecution or punishment of an offence or breach of law
d) for the performance of a contract to which a data subject is party
e) for medical purposes
f) for compliance with a legal obligation to which the data controller is subject.

In all other cases, section 7 (3) gives the data subject the mandate to object to the collection or processing of personal data.

The requirement for consent may also be removed if it is not reasonably practicable to obtain the consent of the data subject.[10]

For children, section 8 requires a data controller or processor to seek consent of the parent/legal guardian before dealing with any data relating to a minor. The known exceptions are if the processing of data is necessary to comply with the law or for research and/or statistical purposes.

These provisions are similar to Article 6(1) 7 & 8 of the GDPR.

It goes without saying that consent must be freely given, specific, informed, unambiguous and without undue influence. in Hall v. Hall LR 1 P&D 481, Sir J. P. Wilde, at p. 482 opines that persuasion is not unlawful, but pressure of whatever character if so exerted as to, overpower the volition without convincing the judgment will constitute undue influence, though no force has been either used or threatened.

[9] Section 7 of the 2019 act provides that personal data may only be collected or processed without consent of the data subject.
[10] Section 11 (g) of the 2019 act.

The concept of undue influence involves one person taking advantage of a position of power over another person. In all cases of undue influence the critical question is whether or not the persuasion or the advice, in other words the influence, has invaded the free volition of the [victim] to accept or reject the persuasion or advice or withstand the influence.

The data subject may be led but must not be driven and the subject's will must be the offspring of his/her own volition, not a record of someone else's. There is no undue influence unless the subject if he/she were free and informed could say "This is not my wish but I must do it."[11]

In Bank of Credit and Commerce International SA v. Aboody [1992] 4 All ER 955, the Court of Appeal classified this doctrine into two types: actual and presumed. Under actual undue

influence the claimant must prove that he or she was induced to sign a contract or agree to a transaction under applied undue influence; whereas in presumed undue influence the claimant only has to prove that there was enough trust and reliance in between the parties that the side committing the wrong abused that relationship by exerting undue influence and inducing them to enter an ambiguous transaction.

Consequently, for consent to be informed and specific, the data subject must be notified about the controller's identity, what kind of data will be processed, how it will be used and the purpose of the processing operations as a safeguard. The data subject must also be informed about his or her right to withdraw consent anytime.

The right to be forgotten

This ability to withdraw consent cannot be divorced from the now established right to be forgotten. The right to be forgotten, was first introduced by the European Court of Justice (ECJ) in a case involving Google Spain,[12] 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.

[11] See Daniel v. Drew [2005] EWCA Civ 507, [2005] WTLR 807 CA at para. 36.
[12] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131

Section 16 of the 2019 act, provides that a data subject may request a data controller to correct, update or destroy/delete personal data if that data is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully.

In Flood v. Times Newspapers Ltd., [2010] EWCA Civ 804, a police officer was accused, in a newspaper article, of taking bribes from Russian exiles with criminal connections. The article was printed in the paper edition of the Sunday Times, and was also made available in its entirety online.

Approximately a year after the article was first published, a report cleared the police officer of any wrongdoing. and held that online archive of a story must be updated to take account of exculpatory developments.

Internet Service Providers (ISPs) can be data controllers or processors and in reconciling Section 16 of the 2019 with Section 29 of the Uganda Electronic Transactions Act, 2011, (ETA) ISPs like all data controllers have a notice and take down requirement.

Section 29 of the ETA reads;
Liability of a service provider
1) A service provider shall not be subject to civil or criminal liability in respect of third-party material which is in the form of electronic records to which he or she merely provides access if the liability is founded on—

a) the making, publication, dissemination or distribution of the material or a statement made in the material; or
b) The infringement of any rights subsisting in or in relation to the material.

Under Section 30 of the ETA, where a service provider refers or links users to a data message
containing an infringing data message or infringing activity, the service provider is not liable for damage incurred by the user if the service provider—

a) does not have actual knowledge that the data message or an activity relating to the data message is infringing the rights of the user;
b) is not aware of the facts or circumstances from which the infringing activity or the infringing nature of the data message is apparent;
c) does not receive a financial benefit directly attributable to the infringing activity; or
d) removes or disables access to the reference or link to the data message or activity within a reasonable time after being informed that the data message or the activity relating to the data message infringes the rights of the user.

In Godfrey v. Demon Internet Limited, [1999] EWHC QB 244, the Queen's Bench found the host of a bulletin board service liable for failing to remove defamatory postings once they were made aware of the content.

In 2015, the European Court of Human Rights (ECHR) in Grand Chamber Case of Delfi AS v Estonia (Application no. 64569/09), departed from the "notice and take down requirement" when it held that an Estonian news site (Delfi) could be held responsible for anonymous and allegedly defamatory comments from its readers even after the
information had been taken down.

Data controllers/processors must therefore put in place mechanisms that make it easy for subjects to request for their data to be forgotten (deleted).

NITA, has the mandate under section 28 of the 2019 Act to order a data controller/processor to delete, update, erase or destroy data of a data subject after receiving a complaint from a subject.

Security

In regards security, the 2019 act provides guidelines for securing data. Section 20 provides that a data controller shall take measures to;

a) Identify reasonably foreseeable internal and external risks to personal data under that person's possession or control;
b) Establish and maintain appropriate safeguards against the identified risks;
c) Regularly verify that the safeguards are effectively implemented; and
d) Ensure that the safeguards are continually updated in response to new risks or deficiencies.

Additionally, under 22 (3) a data controller shall observe generally accepted information security practices and procedures, and specific industry or professional rules and regulations.

What the act does not provide for however, are what appropriate security safeguards are. Rather, it is unequivocal that a data controller should be always vigilant, and ensuring data is secure to the best of his ability. This places a lot of burden on the data controller.

in 1998, the European Commission forwarded a paper[13] on the implementation of Platform for Privacy Preferences (P3P) that tried to reduce this burden by proposing that data protection be between the internet user whose data is being collected and the data controller. If this were implemented it would reduce the influx of cases involving security breaches reported daily.

It is a well settled canon of law that an employer is vicariously liable for the acts of his employees. And, most often than none, it is the employees/contractors of a company that lose data even when state of the art security systems are in place.

It is thus imperative that in addition to the measures above, organizations should follow the interpretative provisions set out in the UK data protection act 1998, Schedule 1, Pt II specifies that where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller should:

[13] Working Party on the protection of individuals with regard to the processing of personal data, European Commission, XV D/5032/98

- choose an organization that offers guarantees about the security of the processing it is undertaking on the organization's behalf;
- put in place a written contract setting out the requirement for appropriate technical and organizational security measures and restricting processing to carrying out the data controller's instructions; and
- Take reasonable steps to ensure compliance with the security measures.

Section 23, of the 2019 act makes it mandatory for a data controller or processor who believes that personal data has been accessed or acquired by an unauthorized person to immediately notify the National Information Technology Authority (NITA). NITA will in turn determine if there's any need to notify the data subject(s).

Cloud computing, IoT & AI

AI or Artificial Intelligence, Is technology that mimics human behavior. AI uses machine learning, where a computer program constantly perfects performing an assigned task by processing massive amounts of data and then identifying and analyzing new data more easily.
The Internet of Things (IoT) is the use of Intelligently connected devices and systems to harness data. This data is gathered by non-intrusive sensors and actuators in machines and other objects which, when connected to the Internet via Wi-Fi, Bluetooth and other networks aggregates data that can be used to improve all facets of life.
The Internet of Things (IoT) essentially brings together advanced software with sensors and other end-devices on a communications network and if used the right way, can lead to a better & transformed Uganda, Africa & the world.

In fact, along with advanced data analytics, IoT-enabled devices and sensors are being used to do things such as diagnose communicable & non-communicable diseases, reduce air pollution, improve crop yield and in large cities, even eliminate traffic jam.

In Spain for example, a citywide WiFi and information network linked to sensors, software and a data analytics platform, enabled the city of Barcelona to provide smart water technology, automated street lighting, remote controlled water irrigation in green spaces and water fountains, "on-demand" waste pickups, digital bus routes, smart parking meters, and more.
Collectively, the result of these IoT-enabled urban services have dramatically reduced traffic congestion and associated pollution as well as water, light and energy usage.
Chicago, in the United States of America is testing a city-wide, edge computing initiative with a network of sensors called "Array of Things" nodes installed throughout city streets. The nodes serve as a sort of "fitness tracker" for the city, collecting data on air quality, climate, traffic and other metrics before sending the information to an open data portal where user groups can consume it for range of applications

In South Korea, the emerging smart city of Songdo is being built around expansive IoT networks designed to ensure its buildings, transportation system and infrastructure are as efficient as possible, helping to optimize its resources.
The IoT can also help cities improve public health. A recent study found dirty air and water led to a staggering 9 million deaths in 2015 alone. For this reason, cities with chronically unhealthy air, such as Delhi in India and Beijing in China, are beginning to utilize sensor networks designed to alert residents when pollution levels are critical .
In London, a city where up to 9,000 deaths per year are attributed to air pollution. London-based Drayson Technologies has been testing the use of networked air quality sensors that are distributed to bicycle couriers and to a fleet of fuel-cell cars. The sensors, which transmit data to smartphones via Bluetooth, allow Drayson to create real-time maps showing air pollution levels around the city.
In Oakland, California, an environmental sensing startup called Aclima, partnered with Google, EDF and researchers from UT Austin to create a highly detailed block-by-block map of air pollution, using a fleet of Google Street View vehicles carrying specialized sensors.

In Energy, Fenix in Uganda launched, ReadyPay Power, an expandable, lease-to-own solar home system that provides lighting, phone charging, TV, and radio, financed to low income homes through affordable installments over MTN mobile money.

In Agriculture which is the backbone of Uganda's technology, IoT can be harnessed to develop smarter ways to increase crop yield and develop more drought resistant crops. In Israel for example, IoT has combined advanced cameras, sensors, weather stations and artificial intelligence, to help farmers respond quickly to signs of trouble such as crop disease, while also boosting productivity by as much as a third.

A professor at the University of California, Davis, Shrini Upadhyaya, devised a wireless sensor system to continuously monitor leaf health, which helps farmers know exactly where and how much they need to irrigate. And throughout rural Africa, startups such as Farmerlineand ArgoCenta are using mobile technology and Big Data platforms to empower smallholder farmers who need access to market data quickly in order to cut waste, improve operations and digitize their supply chains.

In the medical sector, IoT has been used to help doctors gain faster access to health-related data from patients, collected through continuous monitoring and measurement. Wearable, internet-connected sensor devices that track heart rate, pulse, or even blood pressure are increasingly affordable, compact and accurate. While there are serious concerns about how to best safeguard the collection and transmission of this data between patients and their doctors, and how doctors could best leverage it for insights into patients' health trends over time and between checkups, wearables are one of the most promising IoT applications in healthcare.

Increasingly, technology is also helping doctors and other healthcare workers monitor the day-to-day wellbeing of patients who live independently. Sensors mounted throughout the home, or even in-home robotic assistants, can alert caretakers via text if, say, an elderly patient under their care has not taken his medicine on a given day, or left his bedroom by a set time.

In 2015, during the Ebola outbreak in West Africa, Scripps Translational Science Institute eased Ebola detection by using integrated sensors to track heart rate, blood oxygen saturation, respiration rate and temperature.

In cancer treatment, those that detect lumps at the earliest stand a better chance of suppressing the cancer. IoT has been used to track changes in temperature in breast tissue over time through non-intrusive sensors implanted in the breast. The data is transmitted wirelessly to the user's mobile phone and shared securely with a patient's healthcare provider. By applying machine learning and predictive analytics to this data, doctors could identify and classify abnormal patterns indicative of early stage breast cancer.

In Uganda, Malaria is combated with the m-Health application to quickly and cheaply diagnose Malaria using mobile phones. This is a big concern especially with Section 35 that criminalizes the unauthorized disclosure of personal data.

In all the examples provided, the success of such ventures requires leveraging data. Consequently, section 37 of the 2019 Act poses a big threat to AI & IoT as it criminalizes the sale of personal data in whatever form.

For all its successes, the 2019 act may be overshadowed by the ambiguous and ludicrous section 37 that is a stumbling block to the data industry.

The obvious recommendation in this case, would be to remove the clause or provide exceptions like anonymizing data or pushing for consent.

Kenneth Muhangi

Lecturer of Law, Partner- Technology, Media, Telecommunications & Intellectual Property
KTA Advocates

BIBLIOGRAPHY

TEXTBOOKS

1. Bainbridge, David. Introduction to Computer Law, 5th Edition, Pear son Education, UK, 2004.

2. Dickie, John. Internet and Electronic Commerce Law in the Europe an Union, Hart Publishing, 1999.

ARTICLES

1. Adam, Bosnian. 'Cloud Computing', Tolley's practical Audit & Accounting (1st October ,2009)
2. Mark, Turner & Nick Pantlin. 'Financial services in the cloud', Journal of International Banking & Financial Law Volume 26/Issue 2, February 2011.
3. Encyclopedia of Forms and Precedents, 'Data Protection and Free dom of Information Volume' 12(2)
4. Stewart, Room. 'The changing face of data security law', Journal of Privacy and Data Protection, Volume 8, Issue 7, August, 2008.
5. Halsbury's Laws of England, 'The Data Protection Principles, The seventh Data Protection Principle. Confidence and Data protection' volume 8(1)(2003)
6. Mandy, p. Webster. 'Data Security and Outsourcing', Company Secretary's Review, Issue 21, February 2009.
7. Richard, Hollis. 'Data security Part 1 -- five factors leading to Data Compromise Privacy and Data Protection', Volume 10,Issue 2, December 2009
8. Richard, Hollis. 'Data security Part 2 -- five factors leading to Data Compromise Privacy and Data Protection', Volume 10, Issue 3, February, 2010.
9. Tim, Wright & Dominic, Hodgkinson. 'Government response to House of Lords Science and Technology Committee Report on Personal Internet Security' , Computer and Telecommunications Law Review 2008
10. The Economist. 'Is Cloud Computing secure computing?' April 23rd-29th 2011.
11. The Sunday times, December 7 2007.

WEBSITES

1. www.pdpjournals.com
2. www.ico.gov.uk
3. www.data-archive.ac.uk
4. www.dataprotection.gov.uk

LEGISLATION

1. Data Protection & Privacy Act, 2019
2. UK Data Protection Act, 1998
3. Directive 95/46/EEC
4. EU General Data Protection Regulation
5. African convention on Cyber Security and Data Protection

CASE LAW

1. Michael John Durant v Financial Services Authority [2003] EWCA Civ 1746, Court of Appeal (Civil Division)
2. Rhondda BC v Data Protection Registrar (Unreported) 11 October 1991

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