KAA
KAMPALA ASSOCIATED ADVOCATES

Consider it solved

The Data Protection and Privacy Act, 2019;

An analysis of the compliance requirements for data collectors, processors or controllers under the Act.

The act establishes several rights that are to be enjoyed by data subjects in respect of whose personal data is collected or processed.

Introduction

The long awaited and much needed Data Protection and Privacy Bill, 2018 was finally passed into law and assented to by the President on the 25th day of February 2019.
The new Data Protection and Privacy Act, 2019 ("the Act") regulates collection, storage, processing and use of personal data by different entities including government agencies, corporations and private institutions operating both within and outside Uganda.

The Act operationalizes Article 27 (2) of the 1995 Uganda Constitution which guarantees citizens' right privacy. It stipulates that, "no person shall be subjected to interference with the privacy of that person's home, correspondence, communication or other property."
The Act further creates, criminalizes and punishes certain acts which when done, tantamount to offences under the provisions of the law.

Lastly, the Act further tasks the National Information Technology Authority-Uganda ("the Authority") to ensure that the responsible persons/individuals are all compliant with the all the provisions of the Act. This legal alert is therefore intended to inform our clients on the core obligations arising from the Act and to offer guidance to clients on how to strive for compliance with the provisions of the Act.

Interpretation

The Act under the Interpretation section extensively defines a variety of key words that go to the crux of the understanding of the provisions of the new law. While we make no effort as reproducing all the defined words, we have made an effort to select the key definitions for purposes of this alert and these include;

a) **Data** is defined as information which is processed by means of equipment operating automatically in response to instructions given for that purpose.

b) **Personal data** means information about a person from which the person can be identified, that is recorded in any form and includes data relating to nationality, age educational level and identity data among others.

c) **Data subject** means an individual from whom or in respect of whom personal information has been requested, collected, collated, processed or stored.

d) **Data controller** refers to a person who alone, jointly with other persons or in common with other persons or as a statutory duty determines the purpose for and the manner in which personal data is processed or is to be processed.

e) **Data processor** in relation to personal data means a person other than an employee of the data controller who processes the data on behalf of the data collector.

f) **Data collector** means a person who collects.

It is important to note that one of the main features of the Act is the obligation and duty it imposes on persons or bodies that are in the business of collecting, processing and controlling personal data. These include data collectors/processors or data controllers and any other person that holds or uses personal data in their operations.

Secondly, the Act establishes several rights that are to be enjoyed by data subjects in respect of whose personal data is collected or processed.

In doing so, the Act makes data protection and privacy its major concerns as the paramount rights to be preserved.
Therefore, entities that deal in personal data in running their business have to be well conversant with the principles, rights and obligations stipulated under the new Act for each respective party. As these, by virtue of the above definitions are data collectors, controllers and/or processors.
Hence compliance with the provisions of the Act will serve the purpose of preventing the entities/persons from paying hefty monetary fines or custodial sentences imposed by the Act.

What is perhaps more important to note is that, the Act applies across the spectrum, regardless of the mechanism being used for the collection, processing and controlling of the personal data. To that end, it doesn't matter if the personal data is being collected, processed and controlled manually or through the use of Information Communications Technology tools, such as computer systems. As long as personal data is involved, one is automatically brought within the ambit of the Act.

Principles of data protection and privacy

The main objective of the Act is to protect the privacy of data subjects and their personal data. In an effort to fulfill this, the Act establishes certain principles meant to guide the bodies/individuals dealing with personal data. These include:

1) The Act under section 10 prohibits a data controller, data processor or data collector from collecting, holding or processing personal data in a manner that infringes on the privacy of a data subject.

2) Secondly, the Act under section 13 imposes a duty on all data collectors to bring the following information to the attention of a data subject prior to collection of personal data.

- The nature, category and purpose of data to be collected;
- The name and address of the person responsible for collection;
- Whether or not the supply of the data is mandatory or discretionary and the existence of the right to access to and the right to request for rectification of the collected data;
- The recipients of the personal data;
- Consequences of failure to provide the data if any; and
- The period for which the collected data will be retained to achieve the purpose for its collection.

The above information guarantees that only the appropriate and relevant personal data is released to data collectors and most importantly, gives the data subjects an opportunity to make an informed decision, prior to consenting to the collection of the personal data.
Therefore, as a data collector, one must bring to the attention of any data subject the above information prior to obtaining any data from them. Failure of which amounts to an offence. Further, as a precaution, a data collector/controller should endeavor to explain and or translate the above information to a data subject in the manner and language that they are well conversant with.

This in essence takes away room for any misunderstandings and will also help to ensure compliance with the requirements of the Illiterates Protection Act, Cap.78, when dealing with illiterates. In respect of all types of data subjects, it is prudent that, data subjects be given an opportunity to expressly consent, either using a click wrap agreement (for digital platforms) or physical signatures/ thump prints for paper based platforms

It is important to note that the Act under Section 33 (2), states that it shall be a defence in court proceedings where one proves that they took reasonable care in all circumstances to comply with the requirements of the Act.

3) Thirdly, under Section 3, the Act provides principles of data protection to be followed by all data collectors, processors and controllers so as to protect personal data. A data controller, data processor or data controller or any person dealing with personal data shall;

a) be accountable to the data subject for data collected, processed, held or used;

b) Collect and process fairly and lawfully and ensure the quality of the data;

c) Collect, process, use or hold, relevant adequate and necessary personal data;

d) Retain personal data for the period authorized by law or for which it is required;

e) Ensure transparency and participation of the data subject in collection, processing, use and holding of personal data; and

f) Observe security safeguards in respect of the data.
Therefore as a data entity, one must always ensure that they adhere to the above principles when conducting any data related work. This further guarantees to the data subjects that there are governing procedures/guidelines in place to help check their activities in dealing with personal data.

Action steps to be taken by data controllers, processors and collectors.
In an effort to protect and preserve the autonomy and privacy of a data subject, the Act puts in place several action steps to be followed and adhered to by data collectors, controllers or processors. These include:

i) Consent of the data subject

As a general rule section 7 of the Act states that a data collector or processor shall obtain consent of the data subject prior to collecting or processing their personal data. However, the Act provides certain exceptions to this rule. These are;

1. Where such collection or processing is authorized or required by law;
2. Where it's necessary for;
- national security,
- proper performance of a public duty by a public body,
- for the prevention, detection or punishment of an offence or breach of law.
-

3. For the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into the contract;

4. For medical purposes; or
5. For compliance with a legal obligation to which the data controller is subject.

Therefore, it is a mandatory responsibility of data collectors and processors to obtain a data subject's consent prior to collection or processing of your personal data. Unless their acts fall under the ambit of the exceptions enshrined therein.
Every data subject's consent can be obtained using the appropriate means depending on the prevailing circumstances both in the physical and digital world

ii) Personal data relating to children

The Act strictly prohibits collection or processing of personal data relating to a child unless such an act is;

- Carried out with prior consent of the parent or guardian or any other person having authority to make decisions on behalf of the child;
- Necessary to comply with the law; or
- For research or statistical purposes.
-

This safeguards children from data entities who are likely to take advantage of children and extort data from them when unsupervised. Further, children are easily lured and manipulated by adults.
However, for data entities that are engaged in business that involves children they are permitted to collect data of this nature. However, this does not preclude them from adhering to the safety requirements put in place by the Act.

iii) Direct collection of personal data

According to section 11 of the Act, a data collector shall collect personal data directly from the data subject.

However, there are circumstances envisaged under subsection 2 where collection of personal data from another person, source or public body is warranted. These include;

a) where such data is already contained in a public record;

b) the data subject has deliberately made such data public;

c) data subject has consented to the same being collected from another source and is not likely to prejudice the his or her privacy;

d) the collection of data from another is necessary;

- to prevent, detect or prosecute and punish an offence,
- for the protection of national security;
- for the enforcement of legislation which imposes a pecuniary penalty or

e) It is not practicable to obtain the consent of the data subject.

This section goes to show the magnitude of importance the Act attaches to a data subject's autonomy and privacy in respect of their personal data.

Therefore, it goes without saying that for data to be collected from another source, the collector must meet the conditions highlighted in section 11 (2) (e) of the Act. It is imperative to note that, the reading of section 11 (2) (e) of the Act, shows that the collection of personal data from another source may not be appropriate if done by private entities/ individuals for their personal or commercial objectives, as the conditions seem to be strictly limited to public interest objectives..

A data collector should also bear in mind that collection of data from another source doesn't take away his or her responsibility to bring to the attention of such information stipulated under section 13 (1) prior to collection of the personal data except where;

- Information relates to national security;
- Information relating to the enforcement of a law which imposes a pecuniary penalty;
- Information relating to the preparation or conduct of proceedings before a court or tribunal;
- Information relating to enforcement of legislation which concerns public revenue collection; and
- Where it is necessary to avoid the compromise of the law enforcement power of a public body responsible for the prevention, investigation, prosecution or punishment of an offence.

Data controllers, collectors and processors should formulate and create links that automatically send privacy and confidential statements to data subjects as and when their personal data has been collected indirectly.
This serves the purpose of reassuring data subjects of the safe of their personal data however so collected.

iv) Collection for a specific purpose

As a data collector one shall retain and keep personal data for the necessary period to achieve the specific purpose for which it was collected or processed and not any time longer.
It is therefore imperative that every data collector, processor and controller puts in place institutional practices that will ensure that personal data, whose purpose has been achieved or served, is destroyed provided it does not infringe any other statutory requirements such as the Income tax Act.
The above system practices should be secure and of a quality standard. These should be applicable in both the physical and digital space.
Accordingly, there should be a defined data retention policy with defined retention periods known to data subjects in their personal data. The process for the deletion of digital personal data or destruction of physical files containing personal data, should be done using secure methods after completion of stipulated retention period.

v) Specific personal data

The Act under section 9 prohibits the collection and processing of specific personal data. This includes personal data such as;

- that which relates to religious or philosophical beliefs.
- political opinion,
- sexual life and financial information, and
- health status or an individual's medical records.

The exceptions to the above rule include information collected under the Uganda Bureau of Statistics Act, data collected or processed in performance of a statutory imposed obligation on an employer, freely given and with the consent of the data subject and collected in furtherance of legitimate activities of a body or association.
Data collectors and processors who have thus been collecting such data prior to this law and who fall outside the permitted exceptions should stop such practices. Failure of which would amount to the commission of an offence and contravention of the Act.
It is imperative to note that, whereas the Act mentions of the ability to collect such information in furtherance of a legitimate activity, the Act does not however define what 'a legitimate activity' is.

It therefore means that, every organisation ought to consider what their core mandate identity or activities are, before embarking on the collection of any of the specified prohibited personal data. To that end, it is possible for a religious organisation to collection information relating to ones religion while a Political party may be able to collect information on one's political beliefs and not religious belief.

vi) Minimality and quality of information.

Sections 14 and 15, provides that data controllers or processors are only required to process adequate and relevant personal data as authorized by law or required for a specific purpose.
In addition to the above, both data entities and data subjects must ensure that any personal data collected, processed or rendered is complete, not misleading and up to date in respect to the purpose for its collection or processing.

vii) Security Measures

As a data controller/collector or data processor, Part IV of the Act establishes security measures that are to be enforced for purposes of safe guarding personal data of data subjects.
It is important to note that the security measures enacted by the Act refer to both physical and digital security in relation to the personal data, as almost all data entities have both physical and online presence.
Hence in implementing security measures, the data controller, collector or processor should set up such measures that guarantee the safety of their physical space where any personal data (physical and or digital data) maybe held and or stored and also any technological security in respect of information communications systems where personal data in their possession is kept. These include the following;

According to section 20 of the Act a controller/collector or processor shall secure the integrity of personal data that comes into their possession. This can be achieved by adopting appropriate and reasonable measures to prevent loss, damage, unauthorized destruction or unlawful access to and processing of such data.

The security measures to be put in place by a data controller include;
a) Identifying reasonably foreseeable internal and external risks to personal data in one's possession;
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.

Secondly, section 21 tasks data controllers to ensure that **prior to processing any personal data, the data processor has complied with the above highlighted security measures**

While there are no expressly stipulated measures or standards to be followed under the Act, a good starting point for implementing some of the security measures within the digital realm can be borrowed from the National Information Technology Authority of Uganda (NITA-U), Guidelines for Operation, Usage and Management of Information Technology Infrastructure in MDAs & Local Governments. The guidelines provide some practical examples of security measures to include;

Access systems to the location where IT equipment rooms or sites are; installation of alarm systems; installation of security cameras; installation of intrusion detection systems; installation of fire prevention or control measures among other measures. In addition to the above, a data controller shall observe generally accepted information security practices, procedures and specific professional rules and regulations.

The following are some of the generally accepted information security practices and procedures that can be adopted and utilized by data controllers and processors in regard to both physical and digital data;

a) Store hard copies of personal data in locked containers or rooms that are restricted to authorised personnel;
b) Secure configuration for systems and networks;
c) Encrypt personal data transmitted over email AES-128 encryption (using tools like PGP or WinZip) or equivalent standards;
d) Information security incident management;
e) Perform risk assessments on regular basis to identify the risk and likelihood of relevant information security threats (pertaining to confidentiality and integrity);
f) Install licensed hardware/software firewalls on the network/desktops;
g) Configure the firewall with default deny-all rule to block unauthenticated inbound connections;
h) Define a process for granting or revoking physical access to facilities where personal data is stored or processed based on approval from appropriate level of management.
i) Installation of Active Directories with known user access controls and restrictions;
j) Additionally, the visitors once on the premises must be accompanied by data controller, processor or collectors staff and should be easily identifiable (e.g. by using visitor badges) at all times.

viii) Breach of security

Furthermore, in cases where there has been a data security breach through an unauthorized access or acquisition, the data controller/collector or processor should report the incident immediately to the Authority. It will then be the mandate of the Authority to determine whether the data controller/processor or collector should notify the data subject of such a breach. Where the authority deems such notice fit, it shall be done by one of the means stipulated under the Act depending on the prevailing circumstances
While notifying the Authority of the unauthorized access, the data controller/processor or collector should provide sufficient information in relation to the breach.
Notwithstanding the above, certain categories of data subjects such as banks may require a data controller/collector to notify them of a data breach incident in a stipulated time frame.

Hence the data controller/collector should comply with such time frames to avoid breach of their contracts/agreements with the data subject.
Lastly, where the Authority believes that publicity of the above breach will protect the data subject, it shall direct the data controller/processor or collector to publicize the compromise in a specific manner.
Therefore, data controllers, collectors and/or processors should document and implement an Information Security Incident Management plan. This should include the following requirements;

- Definition of information security incidents;
- Roles and responsibilities of the personnel with respect to incident management;

Escalation protocols and contacts for reporting and resolution of information security incidents.In conclusion, the above provision aims at enabling the data subject to devise appropriate mechanisms to safeguard oneself from the consequences of such a breach and prevention of future likelihoods.

i) Rights of data subjects

As the main and primary source of personal data, data subjects enjoy various rights under the Act. The following rights all aim at protecting data subjects and ensuring privacy of their personal data.

a) Access to personal information

Upon proof of one's identity in the manner prescribed by the Act, he or she may request a data controller to grant him or her access to their personal data if any. The request may include confirmation as to whether the data controller has personal data about the particular data subject, the nature of such data and the identity of any third party who has accessed it.

Section 24 mandates the data controller to reject a data subject's request where the information is provided about one's identity and the location of such data is insufficient. This ensures that the person, to whom any personal data is released to, is the right data subject. This also serves as a mechanism to prevent impersonators and fraudsters from accessing other people's personal data.

According to sub section 4, a data controller is precluded from complying with a data subject's request where one can not release the requested data without revealing another individual's data, unless;

- The other individual consents to the disclosure;
- It is reasonable in the circumstances to comply with the request; or
- Compelled by a court order.

The nature of the data referred to above is that which identifies another individual as being the source of any data which the data controller reasonably believes is likely to come into possession of the data subject making the request. However, a data controller shall not use subsection 4 as an excuse to withhold certain information from a data subject making the request which one can release without disclosing another person's identity. He or she should use their expertise to release the data requested for by omitting that which discloses another person's identity.

Lastly, a data controller has thirty (30) days within which he or she should comply with a data subject's request for access to information.
The several qualifiers contained in this section depict the level the act attaches to the privacy and protection of every data subject's personal data as well as third party's information which may be released to another individual.
It is therefore important for data collectors and controllers to invest in systems and processes that will ease the retrieval and access to any such collected and requested personal data to ease compliance with the Act.

b) Right to prevent processing of personal data

A data subject has the right to notify a data controller or processor in writing to stop processing their personal data that causes or is likely to cause unwarranted substantial damage or distress to them at any time
Secondly, a data controller within fourteen (14) days of receipt of the notice, shall inform the data subject that he or she has complied, intends to comply or the reasons for non-compliance. The notice shall be in writing. In cases where the data controller gives reasons for non-compliance, a copy of the notice shall be forwarded to the Authority. The Authority where it is satisfied that a data subject is justified, it shall direct the controller to comply within seven (7) days.

This provision still guarantees a data subject's to right to/control over their personal data even after the point of collection prior to processing.

c) **Right to correct/ delete or destroy personal data (The right to be "forgotten")**

Section 16 allows correction of personal data by data subjects as and when need arises. This provision allows data subjects to put in requests to have their personal data corrected, deleted or destroyed in the possession of data controllers. This is refers to data that may be excessive, out dated or that, whose purpose has since lapsed or the data controller has no right to retain. This has now been called, the ***right to be "forgotten"***.

Where the data controller is unable to meet the data subject's request, the former will inform the latter of its decision and the reasons for the same.
One of the functions the Act gives to the Authority is to order a data controller to rectify, rectify, block, destroy or erase data on the satisfaction of the complaint lodged by the data subject.
It is therefore imperative for data collectors and controllers, to invest in and effective systems and work processes that allow for the deletion or correction of one's personal data, as need be.
Data controllers should also have standard retention policies on a case to case basis upon completion of the purpose for which such data was collected. It is important to note that a data controller/processor should ensure that such policies are not in contravention with statutory legislations on data retention.

Currently Uganda does not have a national data or records retention policy that cuts across the different sectors.
A data retention policy, or records retention policy, is an organization's established protocol for retaining information for operational or regulatory compliance needs. This policy enables the organization's users to systematically organize information to be searched and accessed later or to be disposed off once it ceases to be needed. These policies are executed between the organization and its different customers from whom personal data is to be collected and eventually used.

A good retention policy should include proper data back-up both physical and electronic (such as the cloud). The latter is safer in the event of destruction of the premises.
Further, a data retention policy must consider the value of data over time and the data retention laws an organization may be subject to. In 2006, the U.S. Supreme Court recognized that it is not financially possible to retain all information indefinitely.

However, organizations must demonstrate that they only delete data that is not subject to specific regulatory requirements and use a repeatable and predictable process to do so. This means various types of information are held for different lengths of time. For example, a hospital's retention period for employee email would be different than that of its patient records.
Accordingly, the following are some of the laws that have statutory retention provisions in Uganda for particular data categories;

i) **The Anti-Money Laundering Act, 2013 (AMLA):**

Section 7 of the AMLA requires an accountable person to keep records for a period of 11 years relating to an individual's true identity on whose behalf a business relationship is initiated and for at least ten years after conclusion of such business relations.
The AMLA criminalizes the failure to comply with the above provision.

i) **The Insurance Act, 2017 (I.A):**

Under section 106 (2) of the I.A, licensees and former licensees are required to keep financial statements and other records incident to for at least ten years after the end of the financial year they relate to.
Similarly, failure to comply with the above provision amounts to an offence under the I.A punishable by a hefty fine.
As much as the Authority has the mandate to check and balance the activities of data controllers in respect of retention periods of personal data its powers do not supersede the statutory retention provisions under various legislations.

Rectification, blocking, erasure and destruction of personal data.

In addition to the above, the Authority may order the data controller to rectify, update, block, erase or destroy the data where on the basis of a data subject's complaint, it is satisfied that certain personal data is inaccurate. The above right is applicable whether the data is an accurate record of information received or obtained by the data controller from the data subject or a third party. In case the data is found to be an inaccurate record, the Authority shall direct the data controller to update it with the facts considered to be appropriate. Therefore, once the complained about data has been rectified, updated, erased or blocked, the data controller shall notify the third parties of such an upgrade to whom the data had been previously disclosed.

Accordingly, parties in possession of personal data are able to stay abreast with any updates or variations made to such data as it often changes from time to time. It also saves data entities from running the risk of using and relying on inaccurate or outdated data which may be detrimental to both the entity and the data subject.

d) Right to prevent processing for direct marketing.

The Act under section 26 gives data subjects more power and control over how their personal data is collected and eventually used as well as the right to access of their data. This is meant to prohibit data controllers from using a data subject's data for marketing purposes without obtaining their consent. This provision comes into play where companies collect an individual's personal data for a particular purpose after which they start using such data for marketing purposes without permission to do so.

Direct marketing includes communication by whatever means of any advertising or marketing material which is directed at an individual.
This is common with companies sending unsolicited for promotional/marketing messages to the data subjects. These are often sent by email or telephone numbers.

above information that was not requested for to begin with.
To this end a data subject has the right to request a data controller to stop a data controller from processing their personal data in the circumstances highlighted above
Where a data controller does not comply with the request, the data subject and the authority shall be notified.
The Authority, where it is satisfied with the request, it shall direct a data controller to comply accordingly.
However, it is important to note that a data subject may enter into an agreement with a data controller for use of his or her personal data for pecuniary benefits.
Accordingly, and in the effort not to contravene this provision, companies should include opt-in options in their documents so that data subjects are at liberty to decide whether or not they want to receive promotional information.
Secondly, there is need to include an "unsubscribe" option so that they have the power to decide for how long they wish to receive such marketing information.
Data controllers should desist from presuming that due to the fact that a data subject is receiving a particular service from them, they are interested in the rest of their other services lest they suffer the consequences.

e) Rights in relation to automated decision-making

Under section 27, the Act prohibits the process of making decisions mainly based on automated means without any human involvement. Therefore, the Act puts in place mechanisms to protect data subjects from decisions solely based on automated means by data controllers.
Accordingly, a data subject has the mandate to write to a data controller requiring him to ensure that decisions that significantly affect the former are not only arrived at by automatic means.
However, where a decision that significantly affects a data subject is based solely on automated processing the data controller is obliged to inform the data subject of the same as soon as practicable.

- Through a written notice a data subject has the right to require the data controller to reconsider the automated decision.

The data controller has a time frame of twenty one (21) days

after receipt of the above notice to reconsider their automated decision and inform the data subject in writing and the steps taken or to be taken to comply with the notice.

In circumstances where the data controller efforts in compliance with the data subject's notice are not satisfactory, he or she shall complain to the Authority with fourteen (14) days.

The Authority has the final say in respect of the steps taken by a data controller to comply with data subject's notice.

Despite the above, an automated decision may be made in respect of;

- The process of entry into or performance of a contract with the data subject;
- For a purpose authorized or required by or under any law.

Therefore, as a data controller, one ought to identify the particular decisions that are likely to be based on automatic processing means and;

a) Avail information to data subjects about the automatic processing;
b) Introduce and notify data subjects of simple ways that can be devised to allow human involvement in the decision making, such as grant of access to the automated decision to permit data subjects to review or edit any accuracy issue ;
c) Put in place additional technical and organizational appropriate measures to allow human interaction with the data
d) Inform data subjects about the nature of data used in the decision making;
e) Introduce easy steps of challenging a solely automated decision that significant affects a data subject;
f) Conduct data protection impact assessments (DPIA) before automated means are used for decision making and address any identified issues; and
g) Data controllers should put in place system checks that protect special groups such as children from automated decision making.

Offences and penalties

In its last chapter, the Act creates offences which attract both custodial punishments and monetary fines to be served by any data collector/processor or controller found to be guilty of the offences created therein. These include;

a. Unlawful obtaining or disclosing of personal data;
b. Unlawful destruction, deletion, concealment or alteration of personal data; and
c. Sale of personal data.

The above offences all attract a custodial sentence between ten years and above and or a fine between two hundred and forty currency points and above.

Compensation for damage or distress

Under section 33, a data subject shall be entitled to compensate for the damage or distress occasioned by contravention of the provisions of the Act by a data controller/processor or collector, the responsible party once such a complaint is determined by a court of competent jurisdiction.

Conclusion

The provisions of the Act also extend to data processing that is to be done outside Uganda. In circumstances, the responsible data controller/processor or collector should ensure that such a country has measures in place implemented to ensure protection of such personal data.

The Act is a good step in the right direction yet to be tasted by time. This will also be determined by the efficacy of the Authority and how fast the responsible Minister in conjunction with the Authority will make the enabling regulations to give effect to the Act.

Personal data has been said to be the most valuable resource in the world ahead of oil hence the need to have a good law in place serves the purpose of safeguarding the resource.

As can be discerned, the Act creates various opportunities and challenges for many people. There is however a need for a cultural shift in the work culture, processes and systems on the part of data collectors, processors and controllers. A good starting point however, is for them to invest in numerous technological and physical infrastructural capabilities that will help them attain compliance with the numerous provisions of the Act. In addition, data collectors, processors and controllers need to adopt relevant data collection and retention policies, Security Incident Management Policies among others, which will hopefully guide and inform the manner in which compliance with the Act will be achieved.

Authors

Augustine Idoot Obilil
Partner

Zulaika M. Kasajja
Partner

Patience E. Akampurira
Associate

KAA
KAMPALA ASSOCIATED ADVOCATES

Consider it solved

Consider it Solved

www.kaa.co.ug