Legal Alert

The Data Protection and Privacy Act is here

May 2019

Get in touch

Eeshi Katugugu
Senior Manager
eeshi.katugugu@pwc.com
+256 (0) 312 354 400

This summarises the provisions of the new Data Protection and Privacy Act, 2019 in respect of protection of personal data.

Background

On 28 February 2019, the President assented to the Data Protection and Privacy Act, 2019. The date of commencement is 1 March, 2019. The Act gives effect to Article 27(2) of the Constitution which provides for the protection of citizens' rights to privacy. The Article provides that "No person shall be subjected to interference with the privacy of that person's home, correspondence, communication or other property."

The objective of the Act is to protect the privacy of individuals by regulating the collection and processing of personal information in Uganda and outside Uganda if the information relates to Ugandan citizens; to provide for the rights of the persons whose data is collected and the obligations of data collectors, data processers and data controllers; as well as to regulate the use or disclosure of personal information. The Act gives individuals whose personal information has been requested, collected, collated, processed or stored powers to exercise control over their personal data including consent to the collection and processing, or to request for the correction and deletion of personal data.

The Act is in line with a number of international conventions including; the Universal Declaration of Human Rights to which Uganda is a signatory. It is also in line with the European Union General Data Protection Regulation (GDPR) which gives control to European Union (EU) citizens and residents over their personal data, and applies to every global organisation that may hold or process data on EU citizens and residents.

Application

The Act applies to any person, institution or public body collecting, processing, holding or using personal data within Uganda; and outside Uganda for those who collect, process, hold, or use personal data relating to Ugandan citizens. According to section 2 of the Act, if whatever is being held in any form is enough to identify a particular person then it is personal data. Accordingly, personal data includes nationality, age and date of birth, educational level and occupation, identification number, addresses, email addresses, photographs, telephone numbers, salary details and bank account information, next of kin details, etc. If you or your organisation handle personal information, such as employees records, clients' records etc. you will have a number of legal obligations to protect that information.

The Act defines a data collector as a person who collects data. A data controller is the legal 'person' including the organisation that decides why and how personal data is to be processed. The data controller may appoint another organisation or a person other than an employee of the data controller to be their data processor, in other words to process the data on their behalf. A data subject is an individual from whom or in respect of whom personal data is requested, collected, processed or stored. Typical examples include employees (current and past), interns, casuals, job applicants, suppliers, clients, customers, etc.

Principles of Data Protection

The Act in section 3 outlines seven data protection principles which must be complied with by data collectors, data processors, data controllers or any other person who

collects, processes, holds or uses personal data. These are: accountability to data subjects for data collected; lawfulness, fairness and transparency; adequacy, relevance and minimisation of data collected; data retention only for period authorised by law or purpose; quality and accuracy of data collected, processed, used or stored; transparency and participation of data subjects in collection, processing, use and storage of personal data; and security safeguards in respect of personal data.

Establishment of the Personal Data Protection Office

The Act under section 4 establishes the personal data protection office under the National Information Technology Authority – Uganda (Authority) mandated to, among others oversee the implementation and enforcement of the Act; receive and investigate complaints from data subjects; and establish and maintain a data protection and privacy register.

The Data Protection Officer

The head of every institution that handles personal data is required to appoint a Data Protection Officer. This is the person in the organisation who is the central point of contact and responsible for all data protection compliance issues. For example this would be the person who receives access requests from data subjects, and will also be responsible for making sure that all employees are aware of their data protection responsibilities through induction and training. In addition the Officer will be the main contact for the Authority and will make sure the organisation is registered with the Authority in accordance with section 29 of the Act.

Mandatory Requirements for Collecting and Processing Data

According to section 7, a person should not collect or process personal data without the prior consent of the data subject except where the collection is; authorized by law, for performance of a public duty, for national security, for the prevention, detection, investigation, prosecution or punishment of an offence or breach of law, for medical purposes and for compliance with a legal obligation to which the data controller is subject. Under section 8 prior consent of the parent or guardian of the child shall be sought before collecting or processing personal data relating to a child except where it is necessary to comply with the law or for research and statistical purposes. Section 10 of the Act protects the data subject's right to privacy by prohibiting the collection or processing of personal data in a manner that infringes on the privacy of the data subject. Personal data must be collected directly from the data subject.

Rights of Data Subjects

According to section 24, a data subject who provides proof of identity may request a data controller to give him or her access to the personal information held by the data controller. The data controller is required to comply with the request promptly and in any event not more than thirty days after the request. The data subject has a right to prevent or stop the processing of personal data which causes or is likely to cause unwarranted substantial damage or distress to the data subject by notice in writing to the data controller or processor in accordance with section 25. Section 26 gives a data subject a right to prevent or stop the processing of his or her personal data for purposes of direct marketing. Section 31 gives a data subject a right to make a complaint to the Authority where he or she believes that a data collector or processor or controller is infringing upon his or her right or violating provisions of the Act. A data subject is entitled to compensation for damage and distress caused by the failure of a data controller to comply with the Act.

Offences and Penalties

The Act provides for three types of offences in sections 35 to 37 of the Act, namely;

- unlawfully obtaining, disclosing or procuring the disclosure to another person of personal data held by a data collector, data controller or data processor;
- unlawfully destroying, deleting, misleading, concealing or altering personal data; and
- selling or offering for sale any personal data.

Any person who commits any of the abovementioned offences is liable on conviction to a fine of up to two hundred and forty five currency points (Ugx 4,800,000) or imprisonment not exceeding ten years or both for each category of offence.

Conclusion

Organisations should put in place guidelines and policies for protection of personal data to help them comply with provisions of the Act.

Explicit consent of the data subjects must be sought and obtained by any person or organisation that seeks to collect and process personal data. This is particularly important for employers specifically the human resource departments which regularly collect personal data from employees.

Organisations should review their current practices to establish whether they comply with the Data Protection and Privacy Act, and to assess their internal and external risks. Make sure your organisation's Management and Directors are aware of their responsibilities in respect of Data Protection compliance.

One way for an organisation to ensure compliance with the Act is to decide who will take on the responsibility of checking practices within the organisation, by appointing a Data Protection Officer, preferably an individual with authority within the organisation.

All employees should be sensitized to make sure that they understand their rights and obligations under the Act. Based on the outcome of internal reviews data protection guidelines and a Data Protection Policy should be put in place on how data is collected, processed, stored and retrieved, as well as specifying who will handle data subject access requests. This will then help to ensure consistency and compliance with the Act within the organisation.

Similarly it is important for organisations to make sure that all their service providers have in place enough safeguards to protect personal data from both internal and external risks, and that they maintain acceptable information security practices and procedures to protect personal data.

Organisations should consider reviewing their third party contracts including cloud providers to make sure they are up to required standards.