



Data Protection and Privacy Act of Uganda, 2019

The implications to your organization



Introduction to the Act

On March 1st, 2019, the Data Protection and Privacy Act, 2019 ('the Act') came into force in Uganda.

Definition of data

The Act applies to various categories of persons who may be involved in the flow of data information, including the data subject, data collectors, data processors, and data controllers. It further provides for the rights of data subjects, a data protection register, and offences in the event of a breach of the statutory obligations.

The Act further applies not only to such persons within Uganda, but also those outside the jurisdiction holding information relating to a Ugandan citizen.

This means every company, organization or institution, as long as it collects or processes any data, is subject to this Act.

The Act provides a broad definition of data to include information which is:

- processed by means of equipment operating automatically in response to instructions given for that purpose;
- recorded with the intention that it should be processed by means of such equipment;
- recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system; or
- information not forming any of the above categories but forming part of an accessible record.



Key points to note

-  The Act also borrowed from various international jurisdictions as to how data should be managed. For example, principles surrounding accountability to the data subject for their data, collecting and processing data fairly and lawfully, and observing security safeguards in respect of such data, appear to have been borrowed from the General Data Protection Regulation (GDPR).
-  It is expected that the result of empowering the data subject will be various complaints regarding the misuse of data. The Act has, in fact, created criminal sanctions for unlawful obtaining or disclosing of personal data, unlawful destruction, deletion, concealment or alteration of personal data, and sale of personal data.
-  The data subject may further seek civil remedies in the event of a breach that results in damages. The rights above, enjoyed by the data subject, have invariably become obligations on the data processors, controllers, and collectors.
-  It has, in the past, been commonplace for collectors of information, such as telecommunication companies, to use subscriber information for multiple purposes for which the data subjects did not consent, including, on certain occasions, making the information available to other parties for research purposes, to create their own different packages, marketing, etc.

Establishment of the Personal Data Protection Office:

-  The Act establishes the personal data protection office under the National Information Technology Authority – Uganda (NITA-U) 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.



Data Privacy

Compliance with data protection laws and regulations. Focus on how to collect, process, share, archive and delete data



Data Security

Measures that an organization is taking in order to prevent any third party from unauthorized access



The Data Privacy Officer

The head of every institution that handles personal data is required to appoint a Data Protection Officer. This is the person in the organization 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 NITA-U and will make sure the organization is registered with NITA-U.

Mandatory requirements for collecting and processing Data

1. 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.
2. 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.
3. 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

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.

Offences:

Offences include unlawful obtaining or disclosing of personal data, unlawful destruction, deletion, concealment or alteration of personal data, sale of personal data.

Penalties:

The penalty for any of the above offences by an individual is conviction to a fine not exceeding two hundred and forty-five currency points (UGX 4,800,000) or imprisonment not exceeding ten years or both.

Where an offence listed above is committed by a corporation, the corporation and every officer of the corporation who knowingly and willfully authorizes or permits the contravention is liable to the offence. A court which convicts a person for any of the offences may, in addition to the punishment order the corporation, pay a fine not exceeding two percent (2%) of the corporation's annual gross turnover.

Conclusion

As Grant Thornton Uganda, we recommend that guidelines, policies and practices for protection of personal data should be implemented in each Organization to help comply with provisions of the Act and appoint a Data Protection Officer, preferably someone at a management level.

Explicit consent of the data subjects must be sought and obtained by any person or organization 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.

Organizations 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.

Organizations should also make certain that Management and Directors are aware of their responsibilities in respect of Data Protection compliance.

All customer facing employees should be sensitized to make sure that they understand what is required and expected of them when collecting customer data.

How can we help

Grant Thornton can help you to assess, analyze, identify, develop and deliver the required governance framework, policies, procedures and detailed implementation plan for achieving compliance with the Act.

Services offered by Grant Thornton include:

1. Legal and Regulatory Advice. We can provide you with legal and regulatory advice on how to comply with the Data Protection Act.

2. Record of Personal Data processes activities. We can help you develop a record detailing all processes and systems which collect or process personal data for your organization. This may include departments such as Finance, Human Resources & Administration, Information Technology, Compliance, Operations, Risk Management, etc.

3. Gap Assessment and Implementation Roadmap. We can help you assess your current data policies and practices against the requirements of the act resulting in GAP Assessment Report and an implementation roadmap.

4. Data Protection Framework. We can help you develop a data protection framework that will include the data protection policies and procedures and the data protection governance structures defining the roles and responsibilities.

5. Privacy Notices and Third-Party Contracts. We can help you develop privacy notices for the Data Subjects, Employees, Job Candidates, Third Parties, Customers and the organizations Website.

6. Data Protection Impact Assessment. We can help you to identify and assess high risk personal data processing activities.

7. Awareness and Training. We can provide training to staff and stakeholders to create awareness of the Data Protection Act.



Meet Our Team



Hemal Shah

A qualified Chartered Accountant from ICAI and holds a Bachelors and Masters in Computer Applications and Information Technology. She has over 14 years of rich experience in varied business exposures from ERP implementation to IT audits and valuations.



Ghazali Mohammed

A Computer Scientist with CCNA and CCNP. He has vast experience in IT Infrastructure, cloud migration and IT General Controls testing. He specializes in requirements gathering and analysis, application systems design, networking and administration, IT support.



Author:

Elison Twinomugisha

A Computer Engineer, who is also a Certified Information Systems Auditor (CISA). With rich experience in Systems Audit and Data Privacy. He is responsible for identifying weaknesses in system's network and create action plans to prevent security breaches and possible threats.



Contact details

Address:

2nd Floor, Wing B&C, Lugogo House, Plot 42, Lugogo Bypass,
PO Box 7158
Kampala, Uganda

T +256 200 907333

+256 393 266850

W www.gtuganda.co.ug

E advisory@ug.gt.com

Disclaimer:

This article is developed as an information resource summarising pronouncements issued by the Ministry of ICT & National Guidance. This document is intended as a guide only and the application of its contents to specific situations will depend on the particular circumstances involved. While every care has been taken in its presentation, personnel who use this document to assist in evaluating compliance with applicable laws and regulations should have sufficient training and experience to do so. No person should act specifically on the basis of the material contained herein without considering and taking professional advice. Neither Grant Thornton Uganda, nor any of its personnel nor any of its member firms or their partners or employees, accept any responsibility for any errors this document might contain, whether caused by negligence or otherwise, or any loss, howsoever caused, incurred by any person as a result of utilising or otherwise placing any reliance upon it.



Grant Thornton