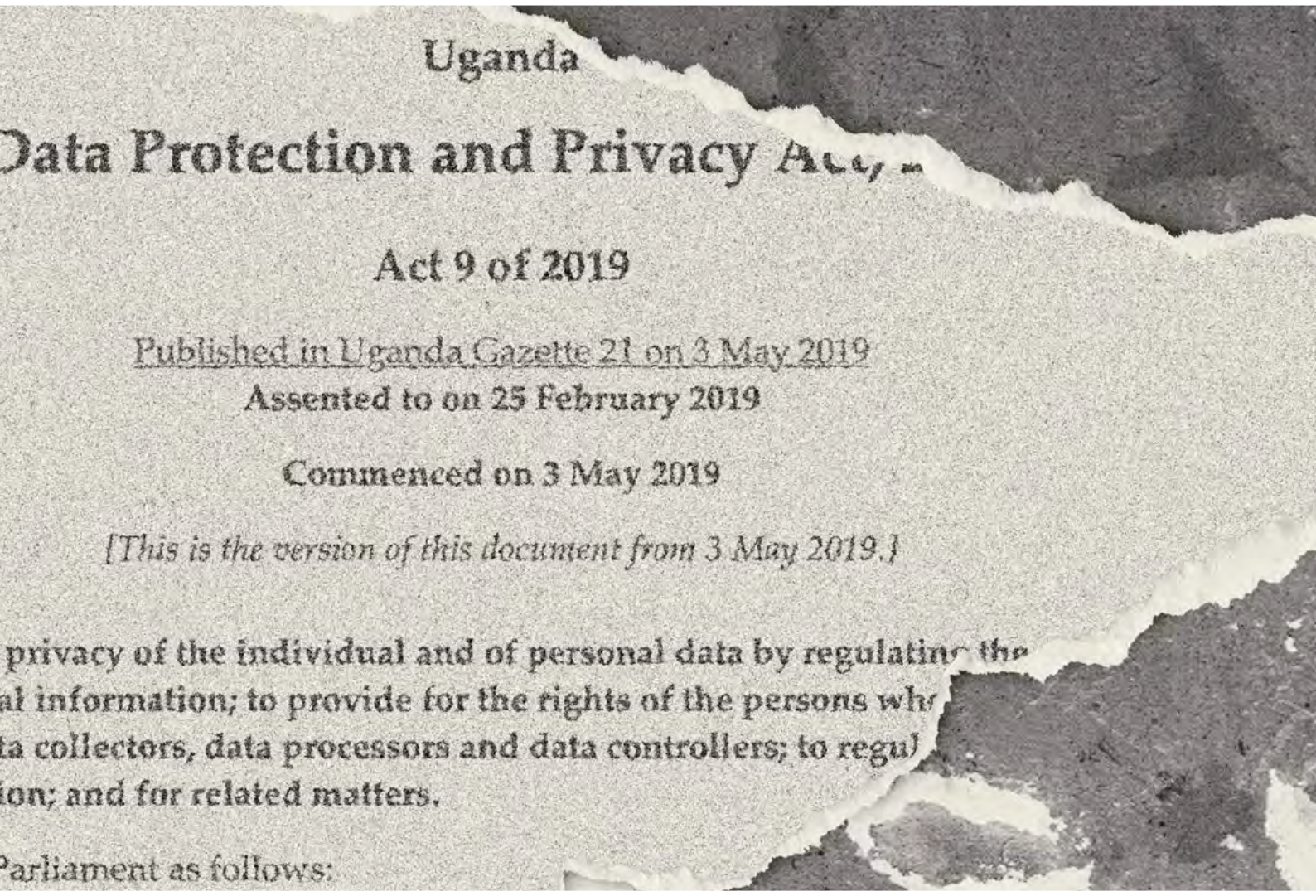
chapter four

PROTECTING CIVIL LIBERTIES &
PROMOTING HUMAN RIGHTS **FOR ALL.**

ISSUE PAPER

DATA PROTECTION LAW & NGOs



An analysis of legal and human rights implications on NGO registration and operations

Issue Paper Number 06/2024

Issue Paper No. 06/2024

Chapter Four Uganda is an independent non-partisan, not-for-profit organization dedicated to the protection of civil liberties and promotion of human rights in Uganda.

TABLE OF CONTENTS

1. INTRODUCTION

Non-Governmental Organisations (NGOs) collect a range of personal data from their data subjects in the course of their formation and operations. They store that data in their records, and in the effort of putting that information to the required use, they process it.

This places them under the ambit of the Data Protection and Privacy Act, 2019 (DPPA)[1] and the Data Protection and Privacy Regulations, 2020 (DPPR).[2]

Data protection laws, such as the DPPA, are important in ensuring respect of the right to privacy. They establish standards and systems that data collectors, processors and controllers must follow. The law further establishes the rights of data subjects, which empowers individuals to control how their personal data is collected, processed, shared and stored.

Data protection refers to the protection of any information relating to an identified or identifiable natural person, including names, date of birth, photographs, video recordings, telephone numbers, email addresses, national identity number (NIN), passport number, etc.

This paper presents an overview of the applicable law standards and key legal obligations that NGOs need to comply with. One of the key obligations under the law is the duty of organisations to register with the Personal Data Protection Office (PDPO) on an annual basis.

Failure to adhere to the stated obligations exposes organisations and individuals to severe sanctions. For example, individuals who unlawfully obtain, disclose, destroy, delete, conceal, alter, or sale personal data face up to ten years imprisonment or a fine of up to Ugx. 4,800,000 or both. NGOs that commit any of the above offences face a fine of up to two percent of the organisation's annual gross turnover.

We hope this paper raises more awareness of the key obligations for NGOs and facilitates discussions on key concerns to avoid misapplication of the law and unintended consequences.

1 The Data Protection and Privacy Act, 2019 [Laws of Uganda]. https://ulii.org/akn/ug/act/2019/9/eng@2019-05-03
2 The Data Protection and Privacy Regulations, 2020.
https://ict.go.ug/wp-content/uploads/2020/08/Data-Protection-and-Privacy-Regulation.pdf

2. HUMAN RIGHTS AND LEGAL ANALYSIS OF UGANDA'S DATA PROTECTION LAW

2.1. Obligation to register with the Data Protection Office

NGOs in Uganda have an obligation to register with the PDPO every year. Under Section 29(2) of the DPPA, the law requires 'every person, institution or public body collecting or processing personal data' to register. During formation of the organisation, recruitment of staff, procurement of services, etc., organisations collect personal data and process it to achieve the desired objective. This personal data often includes names of individuals, information on age, educational level, occupation of individuals, identification numbers, and identity data. The collected data is stored under the custody of the organisation, making the organisation a data controller.

2.2. Overview of principles of data protection

Under the DPPA,[3] NGOs are required to adhere to particular principles of data protection. The principles include the duty to be accountable to the data subject for the data collected from them, collect and process data in a fair and lawful manner, collect and use only relevant data in accordance with the principle of minimality, and retain personal data for a period authorised by law or for a period when the data is required.

NGOs are also required to ensure quality of information collected, processed or held. This seeks to make sure that organisations as data collectors are not processing or holding inaccurate information.

NGOs are further required to ensure transparency and participation of data subjects in the collection, processing, use and holding of the personal data that involves them. In the process of storing the data, the law requires organisations to observe security safeguards in respect of the data. This includes effective use of passwords for information stored digitally or online, safe storage of information in hard copy, among others.

2.3. Data collection and processing standards

The DPPA[4] requires NGOs to adhere to standards of data collection and processing of data in their interaction with personal data. On data collection, the law establishes a general standard that requires that no personal data shall be collected without the prior consent of the data subject. However, there are a few exceptions where data can be collected without consent. The few exceptions include the collection or processing of personal data where the collection or processing is authorised or required by law,

[3] See Section 3 of the Data Protection and Privacy Act, 2019. https://ulii.org/akn/ug/act/2019/9/eng@2019-05-03
[4] See Part III of the Data Protection and Privacy Act, 2019. https://ulii.org/akn/ug/act/2019/9/eng@2019-05-03

where it is necessary for the performance of a public duty, in the interest of national security, for prevention or detection of an offence, for performance of a contract to which the data subject is party, for medical purposes, or for compliance with a legal obligation to which the data controller is a subject.

In all data collection activities, organisations are required to adhere to the principle of minimality which requires that no data shall be processed which is excess of the data required the purpose it was collected for.

NGOs have an obligation to ensure that the data that is collected is 'complete, accurate, up-to-date and not misleading' considering the purpose for which it was collected or processed.

In situations where the organisation needs to process personal data outside Uganda, the law requires the country where the data is going to processed or stored has adequate measures in place for the protection of personal data, at least to the equivalent of Uganda's protection laws. Most organisations are required to pay attention to this obligation because they often process and store data outside of Uganda through the various Google, Zoom, and other related services.

2.4. Standards on data security

The DPPA[5] sets minimum standards on security measures that need to be implemented to ensure that personal data is safe. NGOs are required to ensure that they secure the integrity of personal data in their possession or control by adopting appropriate, reasonable, technical and organisational measures to prevent loss, damage or unauthorised destruction or access of the data.

This legal obligation requires the organisation to conduct internal and external risk assessments to personal data under their control, establish necessary safeguards to the identified risks, ensure effective implementation of the safeguards, and regular updating of the safeguards as risks evolve or new ones emerge.

In the event of a data security breach, the organisation is required under the law to immediately notify the PDPO of the nature of breach and the remedial action taken.

2.5. Rights of data subjects

Data subjects have a number of rights in the exercise of control and protection of their personal data. Under the DPPA,[6] the data subject has a right to access personal information held in the custody of an NGO as a data controller, right to prevent processing of personal data where doing so causes or is likely to cause 'unwarranted substantial damage or distress' to the data subject.

5 See Part IV of the Data Protection and Privacy Act, 2019. https://ulii.org/akn/ug/act/2019/9/eng@2019-05-03
6 See Part V of the Data Protection and Privacy Act, 2019. https://ulii.org/akn/ug/act/2019/9/eng@2019-05-03

Data subjects further have a right to prevent processing of personal data for direct marketing. Under the right to forget, a data subject has a right to request in writing asking the organisation as a data controller to rectify, update, block, erase or destroy the data. If the request is not complied with, the data subject may make a complaint to the Data Protection Office.

Data subjects may request an NGO as a data controller to correct or delete personal data about the data subject where it is 'inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully.'

In the event that the NGO no longer has the authority to retain the data, the data subject can ask the organisation to 'destroy or delete' a record of personal data. Where the organisation is unable to comply with the request, the law requires the organisation to inform the data subject of the rejection and the reasons for the rejection in writing

.

2.6. Offences and penalties

The DPPA[7] establishes a range of offences that carry fines and prison terms.

The first offence, which would expose NGO officers or staff to criminal liability, is unlawful obtaining or disclosing of personal data. This may arise from poor handling of records of data in the hands of the organisation, or deliberate sharing of personal data in your possession without the consent of the data subject. The sanction is imprisonment for ten years or a fine not exceeding Ugx. 4,800,000 or both.

The law provides for the offence of unlawful destruction, deletion, misleading, concealment or alteration of personal data. The sanction is imprisonment for ten years or a fine not exceeding Ugx. 4,800,000 or both.

The law further criminalises the sale or offer for sale of personal data of any person to another. The sanction is imprisonment for ten years or a fine not exceeding Ugx. 4,800,000 or both.

The also provides for offences committed by corporations, including NGOs. Where any of the above offences are committed by the organisation, the organisation may be ordered to pay a fine of up to two percent of the organisation's annual gross turnover.

The law further provides for the criminal offence of failure to comply with a notice issued by the PDPO under the law. Processing or collecting personal data without prior consent of the data subject is also a criminal offence. If someone is convicted on any of these two offences, they face a fine of up to Ugx. 60,000 for each day in default of the notice or to imprisonment of up to six months or both.

[7] See Part VIII of the Data Protection and Privacy Act, 2019. https://ulii.org/akn/ug/act/2019/9/eng@2019-05-03

3. EMERGING LEGAL CONCERNS

3.1. Criminalising informal associations and loose coalitions

The law provides that registration of an organisation as a data collector, data processor or data controller under the DPPA shall be valid for a period of twelve months from the date of registration. This means that the registration certificates under the law expire, which is strange compared to other registration regimes such as incorporation a company, NGO registration, registration with the Financial Intelligence Authority (FIA), among others. It places a further legal restriction and administrative burden on organisations that may prefer to register for five or more years. This legal position exposes many organisations to legal sanctions for operating with expired certificates from the PDPO.

3.2. Vague grounds for possible cancellation of registration

Under the Data Protection and Privacy Regulations, 2020 (DPPR),[8] the PDPO has powers to cancel registration of a data collector, data processor or data controller for any 'good cause' provided they afford a reasonable opportunity to be heard. There are concerns that the phrase 'good cause' is vague and as such provides an overly broad spectrum of interpretation which may be prone to abuse. In the case of *Karamagi and Another v Attorney General (Constitutional Petition No. 5 of 2016) [2023]*, Justice Kakuru, JCC noted, 'a statute is void for vagueness if a legislature's delegation of authority to judges and/or administrators is so extensive that it would lead to arbitrary prosecutions... Vague laws encourage arbitrary and discriminatory enforcement because vague laws delegate enforcement and statutory interpretation to individual government officials.'[9]

3.3. Lack of timeline within which request to erase data must be complied with

The law provides for the right of data subjects to write to data controllers asking for their personal data to be rectified, blocked, erased or destroyed. While this is progressive, the law did not provide for a mandatory timeline within which the requests must be formally responded to. As a result, requests may be ignored for long periods as the personal data so published continues to facilitate a breach of data privacy and other human rights violations.

3.4. Concerns on wide range of fines and prison terms

The law provides for several fines and prison terms in case of non-compliance under the law. There are concerns that these provisions can lead to unintended consequences of an otherwise progressive law. Instead of such punitive measures, the sanctions should require corrective action to promote data protection and where necessary, compensation to data subjects.

8 See Regulation 22. https://ict.go.ug/wp-content/uploads/2020/08/Data-Protection-and-Privacy-Regulation.pdf
9 Link to the full judgment. https://ulii.org/akn/ug/judgment/ugcc/2023/2/eng@2023-01-10

4. CONCLUSION AND RECOMMENDATIONS

4.1. Conclusion

Data protection laws are critical in protecting the right to privacy, particularly in relation to the collection, processing and storage of personal data. The law helps to put in place standards that all data collectors, data processors and data controllers, such as NGOs, should strive to adhere to. However, considering the wide range of legal obligations organisations have to comply with, punitive provisions risk triggering unintended implications on operations of organisations. Data protection is a nascent area of law and legal compliance and many organisations are generally in the initial stages of setting up systems and necessary culture. It is therefore important that sanctions focus on corrective action and encouraging compliance, rather being punitive.

4.2. Recommendations

To the Parliament of Uganda:

- Support the Minister of Information and Communications Technology to effect the amendments detailed in the recommendations below.

To the Minister of Information and Communications Technology:

- Amend Regulation 18 to provide for registration status that does not expire. Registered data collectors, data processors and data controllers should only be required to file annual returns as a measure of monitoring compliance.

- Amend Regulation 22(1) to delete the word 'good cause' and provide for particular grounds under which a registration certificate can be cancelled. The grounds should involve severe and repeated breaches of the law rather than containing general administrative lapses.

- Amend Regulation 37 to provide for a strict time limit within which a request to a data controller to rectify, block, erase and destroy must be complied with / responded to. The timeline provided should be reasonable and in the interest of rights of data subject.

- Repeal the fines and prison terms and provide for corrective actions and where necessary, clauses providing for compensation for data subjects.

To the Personal Data Protection Office (PDPO):

- Scale up awareness raising sessions and enforce the data protection law judiciously to promote corrective action and avoid unintended negative implications on human rights standards.

To Civil Society / NGOs:

- Convene staff trainings to enhance awareness about data protection laws, work to enhance compliance, and advocate for amendments listed above.

Chapter Four Uganda
Plot 2 Wampewo Close, Kololo
P.O Box 33159 Kampala
Phone: +256 200 929 990
Email: info@chapterfouruganda.org
www.chapterfouruganda.org