

Analysis of the Malawi Draft Data Protection Bill, 2021

May 2021

Introduction

The Constitution of Malawi¹ provides for the right to privacy under section 21. The section provides that every person shall have the right to personal privacy, which shall include the right not to be subject to searches of his or her person, home or property; the seizure of private possessions; or, interference with private communications, including mail and all forms of telecommunications.

Malawi is party to several international instruments which provide for the right to privacy, such as the Universal Declaration of Human Rights (article 12), the International Covenant on Civil and Political Rights (article 17), Convention on the Rights of the Child (article 16), and the International Convention on the Protection of All Migrant Workers and Members of Their Families (article 14). Regionally, the right to privacy is stipulated in the African Charter on the Rights and Welfare of the Child (article 19), the African Union Convention on Cybersecurity and Personal Data Protection (which Malawi has neither signed nor ratified)² and the Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019 (principles 40 and 41).³

Malawi has various legislation that impact on digital rights and freedoms including freedom of expression (FoE) and access to information (ATI). These include the Electronic Transactions and Cybersecurity Act of 2016,⁴ which restricts online communications on grounds of protecting public order and national security. Further, section 4(1) of the Official Secrets Act⁵ limits ATI by prohibiting the disclosure of information by public officers, while section 3 of the Preservation of Public Security Act, 1960⁶ penalises the publication of anything likely to prejudice public security or to undermine the government. Further, the Communications Act of 2016,⁷ provides for the interception of communications and, at the same time, prohibits unlawful interception of communications under section 176.

Despite the gaps in the law, data of Malawians has in the past been collected by public and private sector institutions without appropriate safeguards. Mass data collection has been evident through the National Registration and Identification System (NRIS) in which there has been centralised data collection and processing since 2017.⁸ The NRIS is linked to voter registration, revenue collection, immigration, SIM-card registration, banking, as well as financial inclusion and development programmes. Starting March 2021, the system has been used to support the COVID-19 vaccine rollout while at the same time disregarding privacy rights of individuals.⁹

¹ Constitution of Malawi, <https://www.wipo.int/edocs/lexdocs/laws/en/mw/mw030en.pdf>

² African Union, African Union Convention on Cyber Security and Personal Data Protection, Status List, <https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf> (accessed May 10, 2021).

³ Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019, https://www.achpr.org/public/Document/file/English/Declaration%20of%20Principles%20on%20Freedom%20of%20Expression_ENG_2019.pdf

⁴ Electronic Transactions and Cybersecurity Act of 2016, <https://malawilii.org/mw/legislation/act/2016/33>

⁵ Official Secrets Act, https://malawilii.org/system/files/consolidatedlegislation/1401/official_secrets_act_pdf_68659.pdf

⁶ Preservation of Public Security Act, 1960, https://www.policinglaw.info/assets/downloads/1960_Preservation_of_Public_Security_Act_of_Malawi.pdf

⁷ Communications Act of 2016, <https://www.macra.org.mw/?wpdmpromo=communications-act-2016&wpdmdl=10915&refresh=609afd0a9d7d81620770058>

⁸ Tariq Malik, Malawi's Journey Towards Transformation: Lessons from its National ID Project, <https://www.cgdev.org/publication/malawis-journey-towards-transformation-lessons-its-national-id-project>

⁹ See for instance, Jimmy Kainja, Are Malawians Sleep-Walking into a Surveillance State?, <https://cipesa.org/2019/08/are-malawians-sleep-walking-into-a-surveillance-state/>

There have also been public fears of privacy breaches related to the use by the Malawi Communications Regulatory Authority (MACRA) of the Consolidated ICT Regulatory Management Systems (CIRMS) to monitor and analyse telecommunications service performance and quality.¹⁰ While the Malawi High Court found that the system had the potential to facilitate surveillance and violate user privacy and confidentiality of communications, this decision was overturned in 2017 by the Malawi Supreme Court of Appeal, and MACRA subsequently operationalised the system in January 2018.¹¹

Malawi has published the Data Protection Bill, 2021. This analysis highlights the positive and negative aspects of the bill, including its potential impact on freedom of expression, access to information online, and the right to privacy.

The Positives

The Bill will actualise section 21 of the Malawian constitution which has for several years remained largely inoperative due to lack of a specific law that details what the right to privacy entails, and a framework for its enforcement. Enacting the data protection law would represent fulfillment of the state's obligation to protect the right to privacy of the individual and represent a key step towards meeting Malawi's commitments under international human rights law.

The Bill provides for principles governing processing of personal data that could help ensure that individuals' personal data is kept in an accurate, safe, secure, lawful manner and used only within the ambit of the law. The principles include fairness and transparency (**Clause 18**), prohibition of processing of sensitive personal data (**clause 19**), obtaining consent prior to processing data of a minor (**clause 20**), the burden of proof for establishing a data subject's consent being borne by the data controller (**clause 21**), and providing all the necessary information to the data subject prior to direct collection (**clause 22**). Others are data collection based on legitimacy of purpose, data minimisation, retention and accuracy (**clause 23**), conduct of a data protection impact assessment (**clause 24**), measures by data controllers to ensure that other data processors comply with the law, data protection principles, and have appropriate technical and organisational measures to ensure the security, integrity and confidentiality of personal information (**clause 22**).

Under **clause 20** the Bill will guarantee the protection of privacy of children. This is highly reflective of the need to protect vulnerable children from possible abuse by individuals who could unlawfully share, disseminate or sell their personal data.

The data subject's rights, including to obtain one's data from a data controller without constraint or unreasonable delay and at no expense (**clause 26**), to withdrawal consent to processing of personal data (**clause 27**), to object to data processing (**clause 28**), to automated decision making (**clause 29**) and to data portability (**clause 30**) offer protection to the data subjects and give them some level of control over their data and may therefore guarantee some level of data autonomy to the data subjects.

Clauses 34, 35 and 36 are important for portability of data across Malawian borders. Under data portability, the Bill provides for cross-border data transfers, with clause 34 stipulating that data transfers to another country or international organisation are restricted to a recipient "subject to a law, binding corporate rules, contractual clauses, code of conduct or certification mechanism that affords an adequate level of protection".

According to **clause 35**, protection is deemed adequate "if it upholds principles that are substantially similar to the conditions for processing of the personal data" provided for under the Malawian Bill. Among others, adequacy of protection takes into account the availability of enforceable data subject rights; the ability of data subjects to enforce their rights through administrative or judicial redress, and the rule of law generally; the existence of an effective data protection law; the existence and functioning of an independent, competent data protection or similar supervisory authority with adequate enforcement powers; and international commitments and conventions binding on the relevant country or international organisation and its membership of any multilateral or regional organisations.

¹⁰ Gregory Gondwe, 'Spy machine' has great potential of abuse, says court, <https://www.bizcommunity.com/Article/129/15/82204.html>

¹¹ Macra speaks on Cirms, <https://www.mwnation.com/macra-speaks-on-cirms/>

In the absence of adequate protections, cross-border data transfers may only happen if the data subject is informed of the possible risks and consents, if the transfer is necessary for the performance of a contract, or if the transfer is for the benefit of the data subject.

The requirement that controllers and data processors of major importance shall register with the Authority under **clause 37** potentially provides opportunity for control, regulation and checks on the activities of data controllers and processors, which could enhance compliance with the law.

The Negatives

While **Clause 5** exempts processing of personal data to the extent it is carried out by one or more individuals solely for personal, recreational or household purposes from the application of the law, it does not define the terms “personal,” “recreational” or “household” purposes, which could potentially be used to abuse privacy of the data subject. It is therefore important that these terms are defined so as to establish the scope of their application. The full scope of application of the three terms will protect the data subject from unlawful interference.

Clause 8 establishes the Data Protection Office (DPO), which shall be a unit under the Malawi Communications Regulatory Authority (MACRA) established under section 4 of the Communications Act. The Office shall be responsible for the activities of the Authority in relation to data protection under the Act. Given the critical role of the DPO, this proposed structure undermines and limits its financial, decisional and institutional independence. Other countries on the continent, such as Angola, Cape Verde, Ghana, Morocco, South Africa and Tunisia, have established independent Data Protection Commissions to protect the privacy and data of the individual.¹² These commissions have the capacity to act independently in the exercise of their functions. Malawi should therefore consider establishing an independent Data Protection Commission or Authority that is not based within MACRA.

Clause 37 provides for the registration of data controllers and data processors of major importance by the DPO. This clause may be problematic once passed into law. This is because personal data must be protected across all frontiers since there is no data categorised as worth being collected or processed by controllers, nor are there processors that are of less importance. Moreover, the Bill does not specify what amounts to major importance. Under this clause therefore, the term “of major importance” should be deleted so as to promote universal data protection.

Clause 14 provides for a penalty in case of breach of confidentiality of a fine of K5,000,000 (USD 6,289) and imprisonment for five years. This is an express double punishment that may lead to miscarriage of justice. It is also an unusual form of drafting. The provision should therefore be redrafted for the statement to read “and is upon conviction liable to a fine of K5,000,000 or imprisonment for five years or both”.

Similarly, clause 42 also takes away the presumption of innocence which is core to justice processes. The clause provides that, “A data controller or data processor who fails to comply with any order made under sections 40 or 41 commits an offence for which such data controller or data processor is liable to a fine of K5,000,000 and imprisonment for two years.”

The provision should be redrafted as follows:

A data controller or data processor who fails to comply with any order made under sections 40 or 41 commits an offence for which such data controller or data processor is upon conviction liable to a fine of K5,000,000 or imprisonment for two years or both

¹² Piper, D. L. A. “Data protection laws of the world, full handbook.” DLA Piper 1 (2017).



Furthermore, regulation 46(3) has a similar problem. It provides that: “Notwithstanding section 21(e) of the General Interpretation Act, the regulations made under this Act may create offences in respect of any contravention to the regulations, and may for any such contravention impose a fine of up to K5,000,000 and to imprisonment for up to five years.”

The subsection should be redrafted to read as follows:

Notwithstanding section 21(e) of the General Interpretation Act, the regulations made under this Act may create offences in respect of any contravention to the regulations, and may for any such contravention, upon conviction impose a fine of up to K5,000,000 or to imprisonment for up to five years or both.

It should be noted that the penalties provided for are uniform to individual persons and corporate entities. This may not be commensurate with the level of breach especially where data processors and controllers may be able to afford such small fines and therefore continuously engage in personal data breaches. The penalties for corporate entities should therefore be higher and separated from those that individuals may be subjected to.

Lacking Provisions in the Regulations

While the regulations make strides in guaranteeing data protection and privacy of the individual, there are key aspects that are missing in the Bill. Without them, there will be gaps in data protection yet their inclusion will enhance data protection of Malawians. Among the missing aspects which should be included are:

- Arrest with or without warrant which governs the manner in which arrests may be made.
- Seizure of property
- Restoration of Property
- Application for registration of data controllers and data processors
- Prohibition from controlling or processing personal data without registration
- Renewal of Registration
- Changes in details or address of data controllers and processors
- Termination of registration/ Deregistration

Conclusion

The Malawi Data Protection Act is long overdue and the ongoing efforts to legislate data protection are commendable. Malawi’s parliament should therefore, subject to the above proposals, swiftly enact the data protection Bill to provide for protection of rights of individuals. Similarly, the Minister responsible for personal data protection and security should, upon the enactment of the data protection law, swiftly make regulations for the better carrying out of the purposes of the Act.



Collaboration on International ICT Policy for East and Southern Africa (CIPESA)

Tel: +256 414 289 502

Email: programmes@cipesa.org

Twitter: [@cipesaug](https://twitter.com/cipesaug)

Facebook: facebook.com/cipesaug

www.cipesa.org