Ref. No.: **D. 74:05**

Draft: **Data Protection Bill, 2021**

(Subject to Change)

Author: **Macmillan Keck, Attorneys & Solicitors**

Attorneys, Consultants

Date: **14 December 2020**

DATA PROTECTION BILL, 2021

MEMORANDUM

As the Malawi economy becomes increasingly reliant on digital technologies, there is a need to protect personal data of individuals collected, generated, stored and utilized by public and private sector institutions including in the provision of healthcare, health and other types of insurance, education, banking and financial services, hospitality services, civil registration, voting, immigration, national ID and delivery of social programmes.

Such personal data can be stolen, lost, disclosed, misused and abused by those who collect, generate, store and utilize it, resulting in identity theft, unwarranted or embarrassing disclosures, loss of information and unwarranted marketing and solicitation.

In recognition of the dangers posed to individuals by the unregulated or uncontrolled collection and use of personal data and the critical role that the integrity of data, including personal data, plays in the modernization of the Malawi economy, this Bill seeks to provide a comprehensive legislative framework for the protection and security of personal data, consolidate data protection provisions currently found in various Acts of Parliament, and protect the privacy of individuals without hampering social and economic development in Malawi.

The Bill is divided into ten parts.

Part I contains preliminary provisions, namely, the short title of the Bill, the definitions of various terms or expressions used in the Bill and the objectives of the Bill. The overall objective of this Bill is to regulate matters relating to personal data.

Part I also provides for the scope of the application of the Bill. The Bill applies where the data controller or data processor, as defined in the Bill, is domiciled, ordinarily resident, or ordinarily operating in Malawi, is processing personal data withing Malawi, or, subject to some limitations, is processing personal data of a data subject

who is in Malawi. The Bill does not apply to the collection or processing of personal data for personal, recreational or household purposes, or for security, law enforcement or public health purposes.

In Part II, the Bill designates the Malawi Communications Regulatory Authority as the Authority to regulate and monitor personal data protection and privacy in Malawi and oversee the implementation of and be responsible for the enforcement of the Bill. A Data Protection Office is established within the Authority responsible for the activities relating to data protection under the Bill. Part II also described various administrative processes relating to the Authority's data protection duties, functions and powers.

Part III provides for the principles governing the processing of personal data. It requires a data controller or data processor to process data fairly and in a transparent manner and only where (a) the data subject has given and not withdrawn his consent, and (b) the data are required for legitimate purposes outlined in the Bill. The Bill further limits the processing of sensitive personal data. All processing of personal data must adhere to internationally recognized data protection principles set out in Part III.

Part III also requires a data controller or data processor to obtain the consent of a parent or legal guardian where the processing of personal data relates to a person below the age of eighteen years of age. Further, Part III requires a data controller and data processor to carry out a data protection impact assessment where processing is likely to result in high risk to the rights and freedoms of a data subject and to notify the Malawi Communication Regulatory Authority of the results.

Part IV grants a data subject individual rights with respect to personal data, including the right to freely (a) obtain from a data controller or data processor copies of his personal data in a paper-based or commonly used electronic format and demand correction of any inaccurate information or deletion of inaccurate, incomplete

or misleading information, and (b) object, or withdraw his consent previously given, to the processing of his personal data.

Part V deals with data security. It compels a data controller or data processor to implement appropriate technical and organizational measures to ensure the security, integrity and confidentiality of personal data in its possession or under its control, including protection against accidental or unlawful destruction, loss, misuse or alteration and unauthorized disclosure or access.

The Bill sets out obligations of the data controller to report any personal data breaches to the Malawi Communication Regulatory Authority and, where the breach is likely to affect rights and freedoms of individuals, to the data subject.

Part VI restricts a data controller or data processor from transferring personal data from Malawi to another country or international organization except in the circumstances outlined therein.

Part VII provides for the registration of data controllers or data processors of major importance as defined in section 2 of the Bill. The Authority shall maintain a register published on its website of duly registered data controllers or data processors of major importance and prescribe annual fees to be paid by them.

Part VIII deals with provisions for the enforcement of compliance by data controllers and data processors with the requirements of this Bill. It empowers a data subject who is aggrieved by the decision, action or inaction of a data controller or data processor in violation of this Bill and or regulations, rules or other subsidiary legislation or orders to lodge a complaint with the Authority.

Part VIII also obliges the Authority to initiate an investigation on its own accord or upon reference by the data subject in accordance with rules and procedures published in the *Gazette,* and make appropriate compliance and enforcement orders against the violating data controller or data processor. A data controller or data processor who

fails to comply with a compliance or enforcement order is liable a fine of K5,000,000 and imprisonment for two years.

Part IX deals with miscellaneous matters. It provides for exceptions to the application of the obligations and rights under Parts III, IV, V, VI, VII and VIII when a data controller or data processor is processing personal data for the purposes of the prevention, detection or prosecution of criminal offences; promotion of public health or control of epidemic; national security; or is carried out in connection with licensed credit reference bureau under the Credit Reference Bureau Act, Cap. 46:09. Part IX also empowers the Minister responsible for personal data protection and security to make, on the recommendation of the Malawi Communication Regulatory Authority, regulations for the better carrying out of the Bill.

Parliament is informed that in order to implement the mechanics of this Bill and make this Bill the umbrella law on the protection and security of personal data in Malawi, it is necessary to amend or repeal, as the case may be, provisions related to personal data protection in two existing Acts of Parliament, namely, Access to Information Act, 2017 and Electronic Transactions and Cyber Security Act, Cap 74:02. The amendments or repeals will be effected in two separate amending Bills and presented to Parliament simultaneously with this Bill. The proposed amendments and repeals will eliminate inconsistencies between this Bill and the said two Acts of Parliament.

THE DATA PROTECTION BILL, 2021

ARRANGEMENT OF SECTIONS

A BILL

entitled

An Act to make provision for protection of personal data, for regulation of the processing of personal data, and for matters connected therewith or incidental thereto.

ENACTED by the Parliament of Malawi as follows—

PART I—PRELIMINARY PROVISIONS

Short title and commencement

1. This Act may be cited as the Data Protection Act, 2020, and shall come into operation on such date as the Minister may appoint, by notice published in the *Gazette*.

Interpretation

2. In this Act, unless the context otherwise requires—

"Authority" means the Malawi Communications Regulatory Authority established under section 4 of the Communications Act;

Cap 68:01

"binding corporate rules" means personal data protection policies and procedures adhered to by the members of a group of firms under common control with respect to the transfer of personal data among such members and containing provisions for the protection of such personal data.

"biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual, which allow or confirm the unique identification of that individual, including without limitation by physical measurements, facial images, blood typing, fingerprinting, retinal scanning, voice recognition and deoxyribonucleic acid (DNA) analysis;

"certification mechanism" means certification by an official or professional third-party entity that evaluates the personal data protection policies and procedures of data controllers and data processors according to recognised standards;

"consent" means any freely given, specific, informed, and unambiguous indication, whether by a written or oral statement or an affirmative action, of an individual's agreement to the processing of personal data relating to him or to another individual on whose behalf he has the authority to provide such consent;

"data controller" means an individual, private entity, public authority or agency or any other body who or which, alone or jointly with others, determines the purposes and means of the processing of personal data;

"data controller or data processor of major importance" means a data controller or data processor that is domiciled, ordinarily

resident, or ordinarily operating in Malawi and processes or intends to process personal data of more than 10,000 data subjects who are within Malawi, or a greater number of data subjects prescribed by the Authority in rules published in the *Gazette*, or such other class of data controller or data processor that is processing personal data of particular value or significance to the economy, society or security of Malawi as the Authority may designate;

"data processor" means an individual, private entity, public authority or agency or any other body who or which processes personal data on behalf of or at the direction of a data controller or another data processor;

"data subject" means an individual to whom personal data relates;

"personal data" means any information relating to an individual who can be identified or is identifiable, directly or indirectly by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social or economic identity of that individual;

"personal data breach" means a breach of security leading to or reasonably likely to lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

"processing" means any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; and

"sensitive personal data" means personal data relating to an individual's—

(a) biometric data;

(b) race or ethnic origin;

(c) religious or similar beliefs, such as those reflecting conscience or philosophy;

(d) health status;

(e) sex life or sexual orientation;

(f) political opinions or affiliations; or

(g) any other personal data prescribed by the Authority as sensitive personal data pursuant to section 19(2).

Objectives

3. The objectives of this Act are to—

(a) ensure that the processing of personal data complies with principles of data protection, including privacy and data security;

(b) provide individuals with rights with respect to the processing of personal data relating to them;

(c) set standards for the transmission of personal data outside of Malawi;

(d) establish an institutional mechanism to promote and enforce the principles, rights and obligations provided for in this Act; and

(e) provide a legal foundation to promote the digital economy of Malawi and its participation in the regional and global economies through the beneficial uses of personal data.

Application of this Act

4. —(1) This Act applies to the processing of personal data wholly or partly by automated means and processing other than by automated means of personal data which form or are intended to form part of a filing system.

(2) This Act applies only where—

(a) the data controller or data processor is domiciled, ordinarily resident, or ordinarily operating in Malawi;

(b) the processing occurs within Malawi, provided that the mere transiting of data through Malawi shall not constitute data processing occurring in Malawi; or

(c) the processing relates to the targeted offering of goods or services to the data subject in Malawi, or the monitoring of the behaviour of the data subject as far as his behaviour takes place within Malawi.

(3) This Act shall be without prejudice to the application of Part IV of the Electronic Transactions and Cyber Security Act with respect to intermediary service providers and online content editors.

Cap 74:02

(4) For purposes of this section, a "filing system" is a structured set of personal data which are accessible according to specific criteria.

Exemptions

5. —(1) This Act does not apply to the processing of personal data to the extent it is carried out by one or more individuals solely for personal, recreational or household purposes.

(2) Data controllers and data processors that are domiciled, ordinarily resident, or ordinarily operating in Malawi and are not data controllers or data processors of major importance are exempt from the provisions of this Act until the second anniversary of the date on which it comes into force.

PART II— ADMINISTRATION

Duties, functions and powers of the Authority

6. —(1) The Authority shall regulate and monitor personal data protection and privacy throughout Malawi and oversee the implementation of and be responsible for the enforcement of this Act.

(2) Notwithstanding the generality of subsection (1), the Authority shall—

(a) promote public awareness and understanding of personal data protection and the risks to personal data, including the rights granted and obligations imposed under this Act;

(b) promote awareness of data controllers and data processors of their obligations under this Act;

(c) encourage the introduction of technological and administrative measures to enhance personal data security and privacy;

(d) foster the development of personal data security and privacy technologies in accordance with recognized international standards and applicable international law;

(e) participate in international fora and engage with other national and regional authorities responsible for data protection with a view to developing consistent and efficient approaches to regulation of cross-border transfers of personal data;

(f) advise the government on policy issues relating to personal data protection;

(g) submit legislative proposals to the Minister, including amending existing laws, with a view to strengthening personal data protection in Malawi;

(h) collect and publish information with respect to personal data protection, including personal data breaches;

(i) receive complaints relating to violations of this Act or regulations issued thereunder;

(j) conduct investigations of potential violations by a data controller or a data processor of any requirement under this Act or any regulations, rules or other subsidiary legislation or orders made hereunder;

(k) impose penalties in case of violations of the provisions of this Act or any regulations, rules or other subsidiary legislation or orders made hereunder;

(l) designate countries, regions, sectors, international organisations or standard contractual clauses as affording or not affording adequate personal data protection standards for cross-border transfers;

(m) promote competition among entities engaged in the processing of personal data;

(n) ensure compliance with national and international personal data protection standards and obligations laid down by international agreements and treaties to which Malawi is a party;

(o) render technical assistance on personal data protection matters to the Minister;

(p) register and levy fees on data controllers and data processors of major importance;

(q) submit proposals to the Minister for regulations to be made under this Act;

(r) issue directives and opinions, make recommendations and rules and publish guidance as provided under this Act; and

(s) generally implement the provisions of this Act and do all such things as are necessary, incidental or conducive to the better carrying out of the functions of the Authority.

(3) Without prejudice to any functions or powers granted or duties imposed on it under the Communications Act, the Electronic Transactions and Cyber Security Act or any other written law, the Authority shall perform such functions, exercise such powers and undertake such duties as are conferred by this Act.

Cap 68:01

Cap 74:02

Ministerial policy directions

7. —(1) The Authority may, where necessary, seek the general direction of the Minister as to the manner in which it is to carry out its duties under this Act.

(2) The directions given by the Minister under subsection (1) shall be in writing and shall be published in the *Gazette*.

(3) Except as provided for under this Act or any other written law, the Authority shall be independent in the performance of its functions.

The Data Protection Office

8. There is hereby established the Data Protection Office, which shall be a unit under the Authority responsible for the activities of the Authority in relation to data protection under this Act.

Governance powers of the Authority

9. Without prejudice to the generality of section 6, the Authority shall have the power to:

(a) issue guidance, and give directions to the Director General;

(b) approve strategic plans, action plans and budget support programmes submitted by the Director General;

(c) approve annual reports and financial reports submitted by the Director General;

(d) hire consultants to assist the Authority in the discharge of its functions, where necessary; and

(e) issue rules, directives, opinions and make recommendations on any recurrent question related to the regulated missions of the Authority as defined under this Act.

Committees of the Authority

10. —(1) The Authority may for the purpose of performing its functions under this Act, establish committees of the Authority, and delegate to any such committees any of its functions as it considers necessary.

(2) The Chairperson of every committee shall be a person who is a member of the Authority, but an *ex-officio* member shall not be a Chairperson.

(3) The Chairperson of the Authority shall not be a member of a committee.

(4) The Authority shall pay a member of a committee, from the funds of the Authority, an allowance that the Minister responsible for public service may, on recommendation of the Board, approve for attendance at meetings of the committee.

(5) Subject to the general or special directions of the Authority and to the provisions of this Act, every committee of the Authority shall have the power to determine its own procedure.

Advisory fora

11. —(1) The Authority shall establish consultative or advisory fora comprising data controllers and data processors and experts in data protection or another relevant field to assist the Authority with the discharge of its functions under this Act.

(2) The Authority shall contribute out of its annual budget to the expenses of any forum established under subsection (1).

Consultation with other bodies

Cap 74:04

12. —(1) The Authority shall consult and coordinate with the Human Rights Commission established under Chapter XI of the Constitution with respect to the application of this Act and the Access to Information Act and personal data to which both apply.

(2) The Authority shall consult and coordinate with ministries, departments and agencies responsible for the management and regulation of information including personal data in order to promote understanding of this Act, encourage the adoption of good data protection practices and procedures, and resolve any uncertainties about the application of this Act and rules and regulations made hereunder.

Rules of the Authority

13. —(1) In exercise of its functions under this Act, the Authority may make such rules as are necessary for the better carrying out of the provisions of this Act.

(2) The Authority shall consult with relevant ministries, departments and agencies and with data controllers and data processors, interested parties and the public, before making such rules.

(3) The Authority shall publish in the *Gazette* the rules made under this Act.

(4) The Authority shall, within twenty-eight days after the publication in *Gazette* of the rules, inform the public, through the print and electronic media, of the publication of the rules.

(5) Rules made under subsection (1) may prescribe how the provisions of this Act shall apply given the features of any particular use of personal data or any particular sector of the economy or society, including—

(a) health;

(b) education;

(c) financial services;

(d) employment;

(e) electronic commerce;

(f) digital identification;

(g) membership of particular groups and associations;

(h) historical, statistical, journalistic or scientific research; and

(i) any other matter that the Authority may prescribe.

(6) Consultation under subsection (2) shall where appropriate consider the costs and benefits of the proposed rules.

(7) The Authority may publish guidance on good practices and codes of conduct in data protection and compliance with this Act, including the application of data protection principles by design and default in data processing.

Confidentiality

14. —(1) A person shall not publish or disclose to any entity, other than in the course of the entity's duties, the contents of any document, communication or information which has come to the person's knowledge in the course of his duties under this Act.

(2) Any member of the Authority, employee, consultant, adviser or sub-contractor of the Authority who holds confidential information, or any person who has, directly or indirectly, obtained any such information from a member of the Authority, employee, consultant, adviser or sub-contractor of the Authority, whom that person knows or has reasonable cause to believe held the information by virtue of his office, and who—

(a) deals in any contract or proposed contract to which the information relates and in which the Authority is involved;

(b) counsels or instigates anyone else to deal in any such contract or proposed contract, knowing or having reasonable cause to believe that the other entity would deal in such contract or proposed contract; or

(c) communicates to anyone else the information held or, as the case may be, obtained by him if he knows or has reasonable cause to believe that such other entity or any other entity would make use of the information for the purpose of dealing in, or counselling or causing anyone else to deal in, any contract or proposed contract to which the information relates, and in which the Authority is involved,

commits an offence and is liable to a fine of K5,000,000 and imprisonment for five years.

(3) This section shall apply to any information that—

(a) a member of the Authority, employee, consultant, adviser or sub-contractor of the Authority holds by virtue of his office or dealings with the Authority;

(b) would not be expected, or would not be reasonable for it, to be disclosed by a member of the Authority, employee, consultant, adviser or sub-contractor of the Authority except in the proper performance of the functions of his office; or

(c) the member of the Authority, employee, consultant, adviser or sub-contractor of the Authority holding the information knows or ought to know that it is unpublished information in relation to any contract or proposed contract of the Authority.

(4) The provisions of this section shall continue to apply to any member of the Authority, employee, consultant, adviser or subcontractor of the Authority, notwithstanding the expiry or termination of the term of office of the member or the employment of the employee, consultant, adviser or subcontractor of the Authority, as the case may be.

Delegation of powers

15. —(1) The Authority may delegate some of its functions under this Act to the Director General of the Authority, any member of the Authority, the head of the Data Protection Office or any other member of staff of the Authority.

(2) The Director General of the Authority may, with the approval of the Authority, delegate any power or function assigned to him under this Act, to any member of staff of the Authority.

Funds of the Authority

16. —(1) The operational and financial costs of the Authority of carrying out its duties, functions and powers under this Act shall be provided through—

(a) fees, levies and other moneys payable to the Authority under this Act;

(b) fines payable to the Authority in respect of violations of this Act;

(c) grants or donations received by the Authority;

(d) such moneys as are from time to time appropriated to the Authority by Parliament; and

(e) proceeds from the sale by the Authority of any of its assets or equipment to which it has title.

(2) The Authority may charge fees in respect of publications, seminars, documents, and other services provided by the Authority.

Cap. 37:02

(3) Subject to the Public Finance Management Act, the Authority may borrow such amounts as it may require for the performance of its functions under this Act.

(4) The Authority may invest, on short term deposit with any bank or financial institution in Malawi, any of its moneys that are

not immediately required for the performance of its functions under this Act.

Consultations with interested parties

17. —(1) Where the Authority intends to take a decision in accordance with this Act, it shall consult with any interested party, and shall give the interested party an opportunity to comment on the proposed decision within a period specified by the Authority.

(2) The Authority shall publish the results of any consultation launched publicly and the results shall be made available through such means as the Authority considers appropriate in the circumstances, except in the case of information that the Authority considers to be confidential.

PART III— PRINCIPLES GOVERNING PROCESSING OF PERSONAL DATA

Lawfulness of data processing

18. —(1) A data controller shall ensure that personal data is processed, by such data controller or any data processor processing personal data on its behalf, fairly, in a transparent manner and in accordance with subsection (2) and section 19.

(2) A data controller shall neither process nor permit a data processor to process on its behalf, personal data unless—

(a) the data subject has given and not withdrawn his consent;

(b) the processing is necessary 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 a contract;

(c) the processing is necessary for compliance with a legal obligation to which the data controller or data processor is subject;

(d) the processing is necessary in order to protect the vital interests of the data subject or another individual;

(e) the processing is authorised by law and carried out by a competent public authority or agency in furtherance of its legal mandate;

(f) the processing is required by or under any written law or order of a court;

(g) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller or data processor;

(h) the processing is necessary for the purposes of the legitimate interests pursued by the data controller or data processor or by a third party to whom the data is disclosed, except where such interests are overridden by the interests of fundamental rights and freedoms of the data subject;

Cap. 74:04

(i) such processing is necessary to comply with disclosure requirements mandated under the Access to Information Act; or

(j) for the purpose of historical, statistical, journalistic or scientific research.

(3) Further processing of personal data shall be in accordance with the purpose for which the data was collected.

Processing of sensitive personal data

19. —(1) A data controller or data processor shall not process, nor shall it permit a data processor to process on its behalf, sensitive personal data unless—

(a) the data subject has given and not withdrawn his consent to the processing for the specific purpose or purposes for which it will be processed;

(b) the processing is necessary to protect the vital interests of the data subject or of another individual where the data subject is physically or legally incapable of giving consent;

(c) the processing is necessary for the purposes of exercising or performing rights or obligations of the data controller or of the data subject under employment or social security laws or any other written laws designated by the Authority;

(d) the processing is carried out for purposes of medical care or community welfare and is undertaken by or under the responsibility of a professional or similar service provider owing a duty of confidentiality;

(e) the processing is necessary for reasons of public interest in the area of public health;

(f) the processing is necessary for the establishment, exercise or defence of a legal claim or obtaining legal advice;

(g) the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a charitable, educational, literary, artistic, philosophical, religious or trade union aim or whose objective is, in the opinion of the Authority, for the benefit or welfare of the people of Malawi;

(h) the processing is necessary for archiving purposes in the public interest, or historical, statistical, journalistic or scientific research, in each case on the basis of a law, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject; or

(i) the data subject has manifestly made such sensitive personal data public.

(2) The Authority may prescribe in rules published in the *Gazette* further categories of personal data that may be classified as sensitive personal data, further grounds on which they may be processed, and safeguards that may apply, having regard to—

(a) the risk of significant harm that may be caused to a data subject or class of data subjects by the processing of such category of personal data;

(b) the reasonable expectation of confidentiality attached to such category of personal data; and

(c) the adequacy of protection afforded to personal data generally.

Children

20. —(1) When a data subject is below eighteen years of age, a data controller shall obtain consent of a parent or legal guardian of the child to rely on consent under section 18(2)(a).

(2) A data controller or data processor shall apply appropriate mechanisms, including presentation of government approved identification documents, to verify age and consent.

(3) Subsection (1) does not apply to a data controller or data processor when—

(a) the processing is necessary to protect the vital interests of the child; or

(b) the processing is carried out for purposes of medical or social care and is undertaken by or under the responsibility of a professional or similar service provider owing a duty of confidentiality.

Conditions of consent

21. (1) A data controller shall bear the burden of proof for establishing a data subject's consent (or in the case of a data subject below eighteen years of age, the consent of a parent or legal guardian of the data subject) to anything requiring consent under this Act.

(2) In determining whether consent was freely given, account shall be taken of whether performance by a third party of a contract between the data subject and such third party is conditioned on the processing of personal data of the data subject and such processing would not be necessary for such performance.

Provision of information to the data subject

22. (1) When a data controller collects personal data directly from a data subject, the data controller shall provide the data subject with—

(a) the identity of, and means of contacting, the data controller and its representative, if any;

(b) the specific basis of processing under section 18(2) or 19(1) and the purposes of the processing for which the personal data are intended;

(c) third parties with which the data will be shared and where feasible the means of contacting such third parties; and

(d) the existence of the rights of the data subject under Part IV.

(2) When a data controller collects personal data other than directly from the data subject, it must inform the data subject of the

items set out in subsection (1), unless the data subject already has been provided such information or provision of such information is impossible or would involve a disproportionate effort or expense.

Purpose specification, data minimisation, retention and accuracy

23. A data controller shall ensure that personal data is—

(a) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;

(b) adequate, relevant and limited to the minimum necessary for the purposes for which the personal data weas collected or further processed;

(c) retained for no longer than is necessary to achieve the purpose for which the personal data was collected or further processed; and

(d) accurate, complete, not misleading and, where necessary, kept up to date having regard to the purposes for which the personal data was collected or is further processed.

Data protection impact assessment

24. —(1) Where processing is likely to result in high risk to the rights and freedoms of a data subject by virtue of its nature, scope, context and purposes, a data controller shall, prior to the processing, carry out a data protection impact assessment.

(2) The data impact assessment report shall be submitted to the Authority prior to the processing of personal data.

(3) The data controller or data processor shall consult the Authority prior to the processing if, notwithstanding the measures envisaged under subsection (6)(d), the data protection impact assessment indicates that the processing of the data would result in a high risk to the rights and freedoms of the data subject.

(4) The Authority shall publish in the *Gazette*—

(a) guidelines for carrying out data impact assessments; and

(b) lists of the kinds of processing which are, and which are not, subject to the requirement for a data protection impact assessment pursuant to subsection (1).

(5) This section shall not apply until the second anniversary of the date on which this Act enters into force.

(6) For purposes of this section, a "data protection impact assessment" is an assessment of the impact of the envisaged processing on the protection of personal data comprising—

(a) a systematic description of the envisaged processing and its purpose, including where applicable the legitimate interest pursued by the data controller, data processor or third party;

(b) an assessment of the necessity and proportionality of the processing in relation to the purposes the personal data would be processed;

(c) an assessment of the risks to the rights and freedoms of data subjects; and

(d) the measures envisaged to address the risks and the safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Act, taking into account the rights, and legitimate interests of data subjects and other persons concerned.

(7) The Authority may by publication in the *Gazette* exempt categories of data controllers or data processors from the obligations under this section.

Obligations of the data controller and data processor

25. —(1) Where a data controller engages the services of a data processor, or any data processor engages the services of another data processor, the data controller or data processor shall take reasonable measures to ensure that the engaged data processor shall—

(a) comply with the principles and obligations set out in section 23 applicable to the data controller;

(b) assist the data controller or data processor, as the case may be, by appropriate technical and organisational measures, where practical, in the fulfilment of the data controller's obligations to honour the individual rights of data subjects under Part IV;

(c) implement appropriate technical and organisational measures to ensure the security, integrity and confidentiality of personal information as required in Part V, with due regard to section 32;

(d) provide the data controller or data processor, as applicable, with any information it reasonably requires to comply and demonstrate compliance with this Act; and

(e) notify the data controller or data processor, as the case may be, when any new data processors are engaged.

(2) Reasonable measures under subsection (1) include a written agreement between the data controllers and the data processor or between data processors, as the case may be.

(3) The Authority may prescribe such measures in rules published in the *Gazette*.

PART IV—RIGHTS OF A DATA SUBJECT

Rights of the data subject

26. A data subject has the right to obtain from a data controller, without constraint or unreasonable delay and at no expense—

(a) confirmation as to whether or not the data controller, or a data processor operating on its behalf, is storing or otherwise processing personal data relating to the data subject and the source of such personal data;

(b) a copy of such personal data in a paper-based or commonly used electronic format;

(c) correction, or if correction is not feasible or suitable, deletion of any such personal data that is inaccurate, out of date, incomplete or misleading; and

(d) deletion of any such personal data which the data controller is not entitled to retain.

Withdrawal of consent

27. —(1) A data subject has the right to withdraw his consent to processing of personal data under section 18(2)(a) or section 19(1)(a) at any time.

(2) The data controller shall ensure that it is as easy for the data subject to withdraw as to give consent.

Right to object

28. —(1) A data subject has the right to object on grounds relating to his particular situation to the processing of personal data relating to him based on section 18(2)(e) or (h), including profiling, if he can demonstrate that—

(a) such processing is causing or is likely to cause substantial damage or substantial distress to him or to another person; and

(b) such distress or damage is or would be unwarranted.

(2) The data controller may no longer process such data unless it demonstrates a public interest or other legitimate grounds which outweigh any unwarranted distress or damage demonstrated.

Automated decision-making

29. A data subject has the right not to be subject to a decision based solely on automated processing of personal data, including profiling, which produces legal or similar significant effects concerning him, except where such decisions are—

(a) necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) authorized by a written law which establishes suitable measures to safeguard the rights, freedoms and legitimate interests of the data subject; or

(c) authorized by the consent of the data subject.

Data portability

30. —(1) The Authority may make rules and procedures published in the *Gazette* establishing a right of personal data portability.

(2) A right of data portability shall entitle the data subject to:

(a) receive from a data controller personal data concerning them in a structured, commonly used and machine-readable format;

(b) transmit the data obtained under paragraph (a) to another data controller without any hindrance; and

(c) where technically possible, have the personal data transmitted directly from one data controller to another.

(3) The Authority may prescribe the circumstances in, and conditions on, which such a right would apply to a data subject and

the obligations it would impose on a data controller or data processor, or categories of data controllers or data processors, including questions of costs and timing.

PART V—DATA SECURITY

Security, integrity and confidentiality

31. —(1) Each data controller and data processor shall implement appropriate technical and organizational measures to ensure the security, integrity and confidentiality of personal data in its possession or under its control, including protections against accidental or unlawful destruction, loss, misuse or alteration, unauthorized disclosure or access, taking into account:

(a) the amount and sensitivity of the personal data;

(b) the degree and likelihood of harm to data subjects that could result from the loss, disclosure or other misuse of the personal data;

(c) the extent of the processing;

(d) the period of data retention; and

(e) the cost of any technologies, tools or other measures to be implemented relative to the size of the data controller or processor.

(2) Measures implemented under subsection (1) may include:

(a) pseudonymization or other methods of de-identification of personal data;

(b) encryption of personal data;

(c) processes to ensure security, integrity, confidentiality, availability and resilience of processing systems and services;

(d) processes to restore availability and access to personal data in a timely manner in the event of a physical or technical incident;

(e) periodic assessments of risks to processing systems and services, including without limitation where the processing involves the transmission of data over an electronic communications network;

(f) regular testing, assessing and evaluation of the effectiveness of the measures implemented against current and evolving risks identified; and

(g) regular updating of the measures and introduction of new measures to address shortcomings in effectiveness and accommodate evolving risks.

Appropriateness of measures

32. In determining the appropriateness of the measures to be implemented under section 31, a data controller or data processor shall take into account—

(a) available technologies and systems;

(b) the cost of implementing the security measures; and

(c) the relative risks inherent in the nature, scope, context and purposes of the processing and the likely harms to the rights and freedoms of the data subjects.

Personal data breaches

33. —(1) When a personal data breach has occurred with respect to personal data being stored or otherwise processed by a data processor, the data processor shall—

(a) notify the data controller or data processor that engaged it within seventy-two hours after becoming aware thereof, describing the nature of the personal data breach including, where possible, the categories and approximate numbers of data subjects and personal data records concerned; and

(b) respond without undue delay to all information requests from the data controller or data processor that engaged it as they may require to comply with their obligations under this section.

(2) When a personal data breach has occurred with respect to personal data being stored or otherwise processed by a data controller or a data processor acting on its behalf and is likely to result in a risk to the rights and freedoms of individuals, the data controller shall notify the Authority of the breach within seventy-two hours after having become aware of it, describing the nature of the personal data breach including, where possible, the categories and approximate numbers of data subjects and personal data records concerned.

(3) When such a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject—

(a) the data controller shall communicate the personal data breach to the data subject without undue delay in plain and clear language, including advice about measures the data subject could take to mitigate effectively the possible adverse effects of the data breach; and

(b) if a direct communication to the data subject under paragraph (a) would involve disproportionate effort or expense or is otherwise not feasible, the data controller may instead make a public communication in one or more widely-used media sources such that data subjects are likely to be informed.

(4) The notifications and communications referred to in subsections (1), (2) and (3) shall, in addition to the requirements of those subsections, at least:

(a) communicate the name and contact details of a contact point of the data controller where more information can be obtained;

(b) describe the likely consequences of the personal data breach; and

(c) describe the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

(5) The seventy-two-hour period set out in subsections (1) and (2) may be extended to accommodate the legitimate needs of law enforcement or as reasonably necessary to implement measures required to determine the scope of the breach.

(6) The Authority may at any time make a public communication about a data breach notified to it under subsection (2) if it considers the steps of the data controller to inform data subjects inadequate.

(7) In evaluating whether a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject under subsection (3), the data controller and the Authority may take into account—

(a) the likely effectiveness of any technical and administrative measures implemented to mitigate the likely harm resulting from the personal data breach, including any encryption or de-identification of the data;

(b) any subsequent measures taken by the data controller to mitigate such risk; and

(c) the nature, scope and sensitivity of the personal data involved.

(8) The data controller and data processor shall keep a record of all personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken in a manner that enables the Authority to verify compliance with this section.

(9) Where, and in so far as, it is not possible to provide information under this section at the same time, the information may be provided in phases without undue further delay.

(10) This section shall not apply until the second anniversary of the data on which this Act enters into force.

PART VI—CROSS-BORDER TRANSFERS OF PERSONAL DATA

Basis for cross-border transfer of personal data

34. —(1) A data controller or data processor shall not transfer personal data from Malawi to another country or international organisation unless—

(a) the recipient of the personal data is subject to a law, binding corporate rules, contractual clauses, code of conduct or certification mechanism that affords an adequate level of protection with respect to the personal data in accordance with section 35; or

(b) one of the conditions set forth in section 36 applies.

(2) A data controller or data processor shall record the basis for transfer of personal data to another country or international

organisation under section 34(1) and the adequacy of protection under section 35, if applicable.

(3) The Authority may make rules requiring data controllers and data processors to notify it of the measures in place under section 34(1) and to explain their adequacy in terms of section 35, if applicable.

Adequacy of protection

35. —(1) A level of protection is adequate for the purposes of section 34(1)(a) if it upholds principles that are substantially similar to the conditions for processing of the personal data provided for in this Act, including in relation to the onward transfer of personal data to other countries and international organisations.

(2) The adequacy of protection referred to in subsection (1) shall be assessed taking into account:

(a) 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;

(b) the existence of any legally binding instrument between the Authority and a relevant public authority addressing elements of adequate protection referred to in subsection (1);

(c) the access of a public authority to personal data;

(d) the existence of an effective data protection law;

(e) the existence and functioning of an independent, competent data protection or similar supervisory authority with adequate enforcement powers; and

(f) international commitments and conventions binding on the relevant country or international organisation and its membership of any multilateral or regional organisations.

(3) The Authority may from time to time, by notice in the *Gazette*, designate any country, region or specified sector within a country, international organisation or standard contractual clauses as affording or as not affording an adequate level of protection under subsection (1).

(4) The Authority may approve binding corporate rules, codes of conduct or certification mechanisms proposed to it by a data controller, where the Authority determines that the aforesaid meets the adequacy requirements of subsection (1).

(5) The absence of a determination by the Authority under subsection (3) or (4) with respect to a country, territory, sector or international organisation, binding corporate rule, contractual clause, code of conduct or certification mechanism shall not imply the adequacy or inadequacy of the protections afforded by it.

(6) The Authority may make a determination under subsection (3) based on adequacy decisions made by competent data protection

authorities of other jurisdictions where such decisions have taken into account factors similar to those listed in subsection (2).

Other bases for transfer of personal data outside Malawi

36. In the absence of adequacy of protection under section 35, a data controller or data processor shall only transfer personal data from Malawi to another country or international organisation if—

(a) the data subject has given and not withdrawn consent to such transfer after having been informed of the possible risks of such transfers for the data subject due to the absence of adequate protections;

(b) the processing is necessary 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 a contract;

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and a third party; or

(d) the transfer is for the benefit of the data subject and—

(i) it is not reasonably practicable to obtain the consent of the data subject to that transfer; and

(ii) if it were reasonably practicable to obtain such consent, the data subject would likely give it.

PART VII—REGISTRATION AND FEES

Registration of data controllers and data processors of major importance

37. —(1) Data controllers and data processors of major importance shall register with the Authority.

(2) Registration under subsection (1) shall be made by notifying the Authority of—

(a) name and address, or name and address of any representative;

(b) a description of the personal data and the categories and number of data subjects to which the personal data relate;

(c) the purposes for which the personal data is processed;

(d) the categories of recipients to whom the data controller or data processor intends or is likely to disclose the personal data;

(e) the name and address, or name and address of any representative of any data processor operating directly or indirectly on its behalf;

(f) any country to which the data controller or data processor intends, directly or indirectly, to transfer the personal data;

(g) a general description of the risks, safeguards, security measures and mechanisms to ensure the protection of the personal data; and

(h) any other information required by the Authority.

(3) The data controller or data processor of major importance shall—

(a) notify the Authority of any significant change to the information submitted under subsection (2) within 90 days after such change; and

(b) provide the Authority with a full updated registration no later than the third anniversary of its previous registration.

(4) The Authority shall maintain and publish on its website a register of data controllers and data processors of major importance that have duly registered with it under this section.

(5) The Authority shall remove a data controller or data processor from the register if it notifies the Authority that it is no longer a data controller or data processor of major importance.

(6) The Authority may exempt a class of data controller or data processor from the registration requirement of this section where it considers such requirement to be unnecessary or disproportionate.

Fees

38. —(1) The Authority may prescribe annual fees which shall be paid by data controllers and data processors of major importance.

(2) The Authority may prescribe annual fees under subsection (1) applicable to different classes of data controllers or data processors of major importance.

(3) The Government, statutory bodies and any other body appointed by the Government to carry out public functions shall not be subject to the annual fees under subsection (1).

PART VIII—ENFORCEMENT

Complaints

39. —(1) A data subject who is aggrieved by the decision, action or inaction of a data controller or data processor in violation of this Act, subsidiary legislation or orders may lodge a complaint with the Authority in accordance with this Act.

(2) The Authority shall investigate any complaint referred to it where it appears to the Authority that—

(a) the complainant has an interest in the matter to which the complaint relates; and

(b) the complaint is not frivolous or vexatious.

(3) The Authority may initiate an investigation of its own accord where it has reason to believe a data controller or data processor has or is likely to violate this Act or any regulations, rules or other subsidiary legislation or orders.

(4) The Authority may, for the purpose of an investigation, order any person to—

(a) attend at a specific time and place for the purpose of being examined orally in relation to a complaint;

(b) produce such document, record or article as may be required with respect to any matter relevant to the investigation, which the person is not prevented by any other written law from disclosing; or

(c) furnish a statement in writing made under oath or an affirmation setting out all information which may be required under the order.

(5) Where material to which an investigation relates consists of information stored in any mechanical or electronic device, the Authority may require the person named to produce or give access to it in a form in which it is visible and legible in a structured, commonly used and machine-readable format.

(6) The Authority may, where necessary, make representations to the data controller or data processor on behalf of a complainant or to a complainant on behalf of relevant the data controller or data processor, as the Authority may deem appropriate.

(7) The Authority shall establish a section of the Data Protection Office that shall receive and follow up on complaints from data subjects and conduct investigations.

(8) The Authority shall adopt rules and procedures published in the *Gazette* on handling complaints and conducting investigations referred to it under this Act.

(9) A data subject or a recognized consumer organization, or any aggrieved entity, may initiate court action against any data controller or data processor for an offence committed against the data subject, the consumer organization or the entity, provided that the consumer, the consumer organization or the entity has previously filed a complaint with the Authority, and is not satisfied with the decision, or lack of any decision, of the Authority.

Compliance orders

40. Where the Authority is satisfied that a data controller or data processor has violated or is likely to violate any requirement under this Act or any regulations, rules or other subsidiary legislation or orders issued thereunder, the Authority may make an appropriate compliance order against that data controller or data processor.

(2) The order made by the Authority under subsection (1) may include any of the following—

(a) a warning that certain acts or omissions are likely to be a violation of one or more provisions under this Act or any subsidiary legislation or orders issued thereunder;

(b) a requirement that the data controller or data processor complies with such provisions, including complying with the requests of a data subject to exercise one or more rights under this Act;

(c) a cease and desist order requiring the data controller or data processor to stop or refrain from doing an act which is in

violation of this Act, including stopping or refraining from processing personal data that is the subject of the order; or

(d) any other order considered appropriate by the Authority.

(3) An order made under this section shall be in writing and shall specify—

(a) the provisions of this Act that the data controller or data processor has violated or is likely to violate;

(b) in the case of an actual violation, specific measures to be taken by the data controller or data processor to avoid, remedy or eliminate the situation which has resulted in the violation;

(c) in the case of an actual violation, a period not less than 30 days in which to implement such measures; and

(d) in the case of an actual violation, a right to judicial review under section 43.

Enforcement orders

41. —(1) Notwithstanding any criminal sanctions under this Act, if the Authority is satisfied that a data controller or data processor has violated any provision of this Act, or any regulation, rule or other subsidiary legislation made thereunder, any compliance order made under section 40 or any other order made under this Act, it—

(a) may make any appropriate enforcement order or impose a sanction on the data controller or data processor; and

(b) shall inform the data controller or data processor in writing of its decision.

Cap. 1:01

(2) Notwithstanding section 21(e) of the General Interpretation Act, an enforcement order made or sanction imposed under subsection (1) may include the following—

(a) requiring the data controller or data processor to remedy the violation;

(b) ordering the data controller or data processor to pay compensation;

(c) ordering the data controller or data processor to account for the profits made out of the violation;

(d) ordering the data controller or data processor to pay a fine; or

(e) any other order the Authority may deem appropriate.

Offence

42. 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.

Judicial review

43. A person who is not satisfied with an order of the Authority may apply to the High Court within thirty days after the date the order was made for judicial review thereof.

PART IX—MISCELLANEOUS

Exceptions

44. —(1) The obligations and rights under Parts III, IV, V, VI, VII and VIII do not apply to a data controller or data processor when processing of personal data is—

(a) carried out by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;

(b) carried out by competent authorities for the purposes of the promotion of public health or prevention or control of an epidemic;

(c) necessary for national security; or

Cap 46:09

(d) carried out in connection with licensed credit reference bureau business under the Credit Reference Bureau Act;

so long as such processing as is carried out uses suitable measures to safeguard the rights, freedoms and legitimate interests of the data subject.

Joint and vicarious liability

45. —(1) Where a data controller or data processor charged with an offence under this Act is a body corporate, any person who, at the time the offence was committed was a chief executive officer, manager or officer of such body corporate, may be charged jointly in the same proceedings with the body corporate, if the person was party to the offence committed.

(2) A person who is a partner in a firm shall be jointly and severally liable for acts or omissions of other partners in the firm so far as the acts or omissions relate to the firm.

(3) Each data controller and data processor shall be vicariously liable for the acts or omissions of its agent, clerk, servant or other person, in so far as the acts or omissions relates to its business.

Regulations

46. —(1) The Minister may, on the recommendation of the Authority, make regulations for the better carrying out of the purposes of this Act.

(2) Without prejudice to the generality of subsection (1), the regulations may provide for—

(a) the financial management of the affairs of the Authority;

(b) the protection of personal data and data subjects;

(c) the manner in which the Authority may exercise any power or perform any duty or function under this Act;

(d) any matter that under this Act is required or permitted to be prescribed; or

(e) any matter that the Minister considers necessary or expedient to give effect to the objectives of this Act.

Cap. 1:01

(3) 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.

OBJECTS AND REASONS

The principal object of this Bill is to consolidate into a single and effective legislative framework and strengthen the provisions currently found in various Acts of Parliament for the protection and security of personal data used by data controllers and data processors as defined in the Bill in the provision of their services to the public.

CHIKOSA M. SILUNGWE
Attorney General