(Published 2nd February, 2024)

Act

No. 3 of 2024

I assent

Dr. Lazarus McCarthy Chakwera
President
31st January, 2024

ARRANGEMENT OF SECTIONS

SECTION

SECTION

An Act to provide for the protection of personal data of natural persons; the regulation of the processing and movement of personal data of natural persons; the rights of natural persons with respect to the processing of personal data; the obligations of data controllers and data processors; the designation of a Data Protection Authority; and matters incidental thereto

ENACTED by the Parliament of Malawi as follows—

PART I—PRELIMINARY

Short title and commencement

1. This Act may be cited as the Data Protection Act, 2024, 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 which are adhered to by a data controller or data processor or a group of data controllers or data processors engaged in joint economic activity, for a transfer or a set of transfers of personal data to a data controller or data processor outside Malawi;

"biometric data" means personal data resulting from technical processing relating to the physical, physiological or behavioural characteristics of a natural person which confirms the unique identification of that person, and includes, a physical

measurement, facial image, blood type, fingerprint, retinal scan, voice recognition and deoxyribonucleic acid analysis;

"certification mechanism" means certification of personal data protection policies and procedures in accordance with internationally recognized standards, by an official authority or professional third-party entity;

"child" means a person below the age of eighteen years;

"consent" means specific, informed and unambiguous agreement or approval by a natural person, given freely, in writing, orally or by any affirmative action, to a data controller or data processor to process personal data relating to that person or to another natural person on whose behalf the person has the authority to provide the consent;

"data controller" means a natural or legal person who, alone or jointly with another natural or legal person, determines the purpose and means of processing personal data;

"data controller of significant importance" means a data controller who—

(*a*) is domiciled, ordinarily resident, or ordinarily operates in Malawi and processes or intends to process personal data of more than ten thousand data subjects who are resident in Malawi; or

(*b*) processes or intends to process personal data of significance to the economy, society or security of Malawi;

"data processor" means a natural or legal person who processes personal data on behalf of a data controller;

"data processor of significant importance" means a data processor who—

(*a*) is domiciled, ordinarily resident, or ordinarily operates in Malawi and processes or intends to process personal data of more than ten thousand data subjects who are resident in Malawi; or

(*b*) processes or intends to process personal data of significance to the economy, society or security of Malawi;

"data protection officer" means a person designated as such pursuant to section 33;

"data subject" means a natural person to whom particular personal data relates;

"international organization" means an organization governed by public international law and its subordinate bodies, and includes an institution established by, or under, an agreement between two or more countries;

"personal data" means any data relating to an identifiable natural person which, 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 person;

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

"processing" means any operation, or set of operations, performed on personal data, whether or not by automated means, and includes collection, recording, organization, structuring, storage, alteration, retrieval, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data;

"profiling" means any form of automated processing of personal data of a natural person to determine or evaluate certain personal aspects relating to that person, or to analyze or predict aspects concerning the performance of that person at work, or his or her economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

"pseudonymization" means the processing of personal data in such a manner that the data cannot be attributed to a particular natural person without the use of additional information;

"sensitive personal data" means personal data relating to a natural person's—

(*a*) biometric data;

(*b*) race or ethnic origin;

(*c*) religious or other belief relating to the freedom of conscience of the person;

(*d*) health status;

(*e*) political opinion or affiliation; and

(*f*) such other data as the Minister may prescribe; and

"third party" means a natural or legal person other than a data

subject, data controller or processor, who is authorized to process personal data under the direct authority of a data controller or data processor.

Application

3.—(1) This Act shall apply to—

(*a*) the processing of personal data in Malawi by a data controller or data processor domiciled, ordinarily resident or operating in Malawi;

(*b*) the processing of personal data of a data subject who is within Malawi, by a data controller or data processor who is domiciled, ordinarily resident or operating outside Malawi, and the data processing relates to the—

(i) offering of goods or services, irrespective of whether the data subject is required to pay for the goods or services; or

(ii) monitoring of the behavior of the data subject, as far as the behaviour takes place within Malawi; and

(*c*) the processing of personal data in Malawi, whether wholly or partly by automated means or by other means other than automated means, which forms or is intended to form part of a filing system.

(2) This Act shall not apply to—

(*a*) the processing of personal data by a natural person in the course of performing a solely personal, recreational or household activity; and

(*b*) the mere transmission of personal data through Malawi.

(3) This Act shall not affect the rights and obligations of a data controller and data processor prescribed under Part IV of the Electronic Transactions and Cyber Security Act.

Cap.74:02

(4) For the purposes of this section—

(*a*) "household activity" means correspondence, the holding of addresses, social networking and any other online activity undertaken within the context of a household activity; and

(*b*) "filing system" means any structured set of personal data which is accessible by reference to a data subject or according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.

Part II—Administration

Designation of Data Protection Authority

4.—(1) The Malawi Communication Regulatory Authority (hereinafter referred to as the "Authority") is hereby designated as the Data Protection Authority.

(2) The Authority shall perform its functions and exercise the powers provided for under this Act independent of the direction, influence or interference of any person or entity.

Functions of the Authority

5.—(1) The Authority shall regulate the processing of personal data as prescribed under this Act and oversee the implementation, and be responsible for the enforcement, of this Act.

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

(*a*) develop and publish guidelines on data protection to promote data protection and compliance with this Act;

(*b*) promote public awareness of this Act and international personal data protection legal frameworks;

(*c*) encourage the development and introduction of personal data protection technologies and administrative measures, in line with international standards and applicable international laws;

(*d*) engage with national, regional and international authorities responsible for data protection to develop consistent and efficient approaches to the regulation of cross-border transfer of personal data;

(*e*) advise the Minister on policy issues relating to personal data protection;

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

(*g*) keep and maintain a register of data controllers of significant importance and data processors of significant importance; and

(*h*) do all such acts and things as are necessary or incidental to the implementation of this Act.

Powers of the Authority

6. The Authority may—

(*a*) designate a country, region or sector as affording adequate personal data protection standards for cross-border transfers pursuant to section 39;

(*b*) prescribe and approve standard personal data protection contractual clauses;

(*c*) issue compliance orders in cases where this Act is contravened; and

(*d*) do all such acts and things as are necessary or incidental to the implementation of this Act.

Advisory committees

7.—(1) The Authority may establish such number of advisory committees, as the Authority determines necessary, to advise the Authority in the discharge of its functions under this Act.

(2) An advisory committee established under subsection (1) shall comprise—

(*a*) a representative of data subjects;

(*b*) a representative of data controllers;

(*c*) a representative of data processors;

(*d*) an expert in data protection; and

(*e*) such other experts from any other relevant field as the Authority may determine.

(3) The Authority shall designate one of its members, other than an *ex-officio* member, as chairperson of a committee established under subsection (1).

(4) An advisory committee shall act in accordance with the mandate and any directions given to it, in writing, by the Authority.

(5) The terms and conditions applicable to members of a committee of the Authority established under the Communications Act shall apply to members of an advisory committee established under subsection (1).

Cap. 68:01

(6) The Director General of the Authority shall act as secretary to an advisory committee established under subsection (1) or may, with the approval of the Chairperson of the Authority, delegate a senior member of staff to act as secretary to the advisory committee.

Part III—Principles Relating to the Processing of Personal Data

Personal data to be processed lawfully, fairly, etc.

8.—(1) A data controller and data processor shall process personal data lawfully, fairly and in a transparent manner.

(2) The processing of personal data shall be lawful if—

(*a*) the data subject provides consent to a data controller or data processor to process the data for one or more specific purposes or, where the data subject has no capacity to provide consent, another natural person who has authority to provide consent on behalf of the data subject provides the consent; or

(*b*) the processing of the data is—

(i) necessary for the performance of a contract to which the data subject is a party or, at the request of the data subject prior to the data subject entering into the contract;

(ii) a legal requirement or obligation of the data controller or data processor;

(iii) necessary in order to protect vital interests of the data subject or another natural person;

(iv) authorized by a written law and carried out by a competent public authority in furtherance of its legal mandate;

(v) required by, or under, any written law or an order of a court of law;

(vi) 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; or

(vii) necessary for the purpose of a legitimate interest pursued by the data controller or data processor or by a third party to whom the data is disclosed, except where the interest of the data controller or data processor or third party is overridden by the interest of a fundamental right or freedom of a data subject.

Purpose limitation

9.—(1) A data controller and data processor shall collect personal data for a specific and legitimate purpose and shall not process the data in a manner that is incompatible with the purpose for which it was collected.

(2) A data controller or data processor who intends to process personal data for a purpose other than the purpose for which the data was originally collected, shall ascertain whether the processing of the data for the other purpose is compatible with the purpose for which the data was initially collected.

(3) A data controller or data processor shall, in ascertaining compatibility under subsection (2), consider—

(*a*) any linkage between the purpose for which the data was originally collected and the other purpose for which the data controller or data processor intends to process the data;

(*b*) the context in which the data was originally collected, in particular, having regard to the relationship between a data subject and the data controller;

(*c*) the nature of the data to be processed, in particular, having regard to the sensitivity of the data;

(*d*) potential consequences of the intended data processing to the data subject; and

(*e*) the existence of appropriate safeguards, including encryption and pseudonymization.

(4) Where a data controller or data processor subsequently processes personal data, for the purpose of archiving the data for public interest or for research or statistical purposes, the subsequent processing of the data shall not be considered to be incompatible with the original purpose for which the data was collected.

Data minimization

10. A data controller and data processor shall ensure that personal data intended to be processed by the data controller or data processor is adequate, relevant and limited to what is necessary for the purpose for which the data is intended to be processed.

Data accuracy

11.—(1) A data controller or data processor shall ensure that the personal data the data controller or data processor intends to process is accurate and, where necessary, is up-to-date.

(2) Where a data controller or data processor intends to process personal data and it comes to his or her knowledge that the data is inaccurate, in relation to the purpose for which it is intended to be processed, the data controller or data processor shall erase the data or take steps to rectify the inaccuracy.

Storage limitation

12.—(1) A data controller and data processor shall not store personal data for a period that is longer than the period that is necessary to achieve the purpose for which the data is processed.

(2) A data controller and data processor may store personal data for a period longer than the period prescribed under subsection (1) where the data is stored for the purpose of archiving for public interest or for research or statistical purposes.

(3) Where the data controller or data processor stores personal data in accordance with subsection (2), the data controller or data processor shall ensure that—

(*a*) the principle of data minimization, as provided under section 10, is adhered to; and

(*b*) the personal data is, where appropriate, pseudonymized.

Data integrity and data confidentiality

13.—A data controller and data processor shall ensure that the appropriate technical or organizational security measures are implemented to guarantee the security of personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction, or damage of the data.

Principles for determining the validity of consent

14.—(1) A data controller shall—

(*a*) obtain the consent of a data subject; or

(*b*) where the data subject is a child or a person who is not capable of providing consent, obtain the consent of the legal guardian of the data subject,

before processing the personal data of the data subject.

(2) Where a data controller seeks consent from a data subject on several matters in the form of a written declaration, each matter on which consent is sought shall be presented in a clearly distinguishable manner.

(3) A data subject may, at any time, withdraw consent given to a data controller and the withdrawal of the consent shall, where practicable, be in the same manner the consent was provided.

(4) Where a data subject withdraws consent in accordance with subsection (3), the withdrawal shall not affect the legality of the data processing that occurred before the withdrawal of the consent.

(5) Where a question arises on whether consent was freely provided, consideration shall be taken of whether the performance of a contract between the data controller and the data subject or the delivery of a good or a service by the data controller to the data subject is conditional on provision of the consent.

Provision of information to a data subject

15.—(1) A data controller who collects personal data from a data subject shall, at the time of collecting the data, provide the following information to the data subject—

(*a*) the identity and contact details of the data controller or representative of the data controller;

(*b*) the legal basis for processing the personal data;

(*c*) the purpose for processing the personal data;

(*d*) where possible, the storage period for the personal data;

(*e*) the existence of automated decision-making, including profiling;

(*f*) the rights of the data subject provided under Part IV;

(*g*) the right to lodge a complaint with the Authority under section 44; and

(*h*) whether the data controller intends to transfer the personal data to a place outside Malawi.

(2) Where a data controller obtains personal data of a data subject from a person other than the data subject, in accordance with any of the grounds under section 8(2)(*b*), the data controller shall, within fourteen days of obtaining the personal data, provide the information specified in subsection (1) to the data subject.

Processing of sensitive personal data

16.—(1) A data controller and data processor shall not process sensitive personal data of a data subject unless—

(*a*) the data subject has provided consent to the processing of the data for a specific purpose;

(*b*) the processing of the data is necessary to protect the interest of the data subject;

(*c*) the processing of the data is necessary for the purpose of exercising or performing a right or obligation of the data controller, data processor or data subject under a written law or a court order;

(*d*) the processing of the data is in the interest of public health;

(*e*) the processing of the data is for public interest;

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

(*g*) the processing of the data is necessary for the purpose of archiving the data for public interest or for research or statistical purposes;

(*h*) the data subject has intentionally made the data public; or

(*i*) the data controller or data processor is a foundation, association or any other not-for-profit body with a charitable, educational, literary, artistic, philosophical, religious or trade union aim and the data processing is carried out in the course of implementing a legitimate activity of the data controller or data processor to its members or former members or to a natural person who is in regular contact with the data controller or data processor, in connection with its purposes.

(2) Where sensitive personal data is processed in accordance with subsection (1), the data controller or data processor shall put in place appropriate measures to safeguard the fundamental rights and interests of the data subject.

(3) The Minister may, in addition to the categories of personal data specified as sensitive data under section 2, on the recommendation of the Authority and by order published in the *Gazette*, prescribe additional categories of personal data to be classified as sensitive data.

Processing personal data of children and other legally incapacitated persons

17.—(1) Where a data subject is a child or any other natural person lacking the legal capacity to exercise the rights of the data subject prescribed under this Act, a parent or legal guardian, as the case may be, of the data subject shall exercise the rights of the data subject on behalf of the data subject.

(2) Where the legal basis for processing personal data is consent, pursuant to section 8(2)(*a*), a data controller or data processor who

intends to process personal data of a data subject who is a child or any other natural person lacking legal capacity to provide consent shall obtain the consent from a parent or legal guardian, as the case may be, of the data subject.

(3) A data controller or data processor who obtains consent in accordance with subsection (2) shall put in place appropriate mechanisms to verify the age of the child or the mental capacity of the other natural person, as the case may be, and the identity of the parent or legal guardian providing the consent.

Processing of personal data relating to criminal offences, convictions, etc.

18.—(1) Without prejudice to section 8(2), a data controller or data processor shall not process personal data of a data subject relating to a criminal offence, conviction, or security measure imposed on the data subject unless—

(*a*) the processing is authorized by a written law and the law provides for the necessary safeguards for the rights and freedoms of the data subject; or

(*b*) the processing is carried out under the control of an organ of Government or other official authority.

(2) For purposes of this section "organ of Government" means the three branches of Government, a local authority and a body or a committee established or instituted by, or under, any written law.

Part IV—Rights of a Data Subject

Right to access personal data

19.—(1) A data subject has the right to obtain from a data controller or data processor, confirmation of whether personal data concerning the data subject is being processed by the data controller or data processor, and where that is the case, the right to access the personal data being processed.

(2) Where the data controller or data processor confirms the processing of the personal data of the data subject, the data controller or data processor shall provide the data subject with—

(*a*) on demand, a copy of the personal data being processed—

(i) in a commonly used electronic format;

(ii) within thirty days of receipt of the request; and

(iii) where practicable, at no expense to the data subject; and

(*b*) information specified in section 15(1).

Right to data portability

20.—(1) A data subject has the right to receive personal data concerning the data subject from a data controller in a structured, commonly used and machine-readable format where the processing of the personal data is—

(*a*) based on consent pursuant to sections 8(2)(*a*) or 16(1)(*a*) or fulfilment of a contractual obligation pursuant to section 8(2)(*b*); or

(*b*) carried out by automated means.

(2) A data controller shall, on request by a data subject—

(*a*) provide to the data subject personal data of the data subject in a commonly used and machine-readable format; or

(*b*) transmit personal data of the data subject directly to another data controller specified in the request,

within thirty days of receipt of the request.

Right to rectification of personal data

21.—(1) A data subject has the right to rectify any error in personal data of the data subject collected by or being processed by a data controller or data processor.

(2) A data subject has the right to have his or her incomplete personal data completed.

(3) A data controller or data processor who receives—

(*a*) a request from a data subject to rectify an error in the personal data of the data subject; or

(*b*) supplementary data from a data subject aimed at completing personal data of the data subject that is incomplete,

shall rectify the error in the personal data or add the supplementary data to the personal data of the data subject, within fourteen days of receipt of the request or the supplementary data.

Right to erasure of personal data

22.—(1) A data subject has the right to erasure of personal data concerning the data subject, without undue delay, where—

(*a*) the personal data is no longer necessary in relation to the purpose for which the data was processed;

(*b*) the data subject withdraws the consent on which the processing of the personal data is based and there is no other legal ground for processing the data;

(*c*) the data subject objects to the processing of the personal data pursuant to section 24 and that there is no overriding legitimate ground for processing the data;

(*d*) the personal data has been unlawfully processed; or

(*e*) there is a legal obligation under a written law to erase the personal data.

(2) A data controller or data processor who receives a request from a data subject to erase personal data of the data subject in

accordance with subsection (1), shall take reasonable steps to inform other data controllers and data processors who, to his or her knowledge, are processing the data to adhere to the request of the data subject.

Right to restriction of processing personal data

23.—(1) A data subject has the right to restrict the processing of personal data of the data subject where—

(*a*) the accuracy of the data is contested by the data subject; or

(*b*) the data controller or data processor no longer needs the data for the intended purpose of processing.

(2) A data controller or data processor who receives a request from a data subject to restrict processing of personal data of the data subject, in accordance with subsection (1), shall adhere to the request, unless the data controller or data processor shows cause, in writing, why the request cannot be adhered to.

Right to object

24.—(1) A data subject has the right to object to the processing of personal data of the data subject at any time, where the processing of the data is pursuant to section 8(2)(*b*) (vi) or (vii)—

(*a*) the processing is causing, or is likely to cause, substantial damage or substantial distress to the data subject; and

(*b*) the damage or distress referred to in paragraph (*a*) is, or would be, unwarranted.

(2) A data controller or data processor shall, upon receipt of an objection from a data subject under subsection (1), cease to process the personal data, unless the data controller or data processor, as the case may be, demonstrates that—

(*a*) there is a compelling legitimate ground for the processing which overrides the interest or right of the data subject; or

(*b*) the processing is necessary for the establishment, exercise or defence of a legal claim.

(3) A data subject may, where the personal data of the data subject is processed for a direct marketing purpose, object to the processing of the data for that purpose.

Automated decision-making

25.—(1) 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 a legal or similarly significant effect concerning the data subject.

(2) Subsection (1) shall not apply where the decision is—

(*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 has suitable measures to safeguard the rights and interests of the data subject; or

(*c*) based on the consent of the data subject.

(3) Where an exception under subsection (2) applies, a data controller shall implement the appropriate measures to safeguard the rights and interests of the data subject.

Derogations

26.—The rights of a data subject provided under this Part may be restricted where the processing of the personal data of the data subject is for the purpose of—

(*a*) national security, including safeguarding against and the prevention of a threat to national security;

(*b*) the prevention, investigation, detection or prosecution of a criminal offence or the execution of a criminal penalty;

(*c*) pursuing a national economic or financial interest, including a monetary, budgetary and taxation matter;

(*d*) public health;

(*e*) social security;

(*f*) judicial proceedings;

(*g*) the prevention, investigation, detection and prosecution of a breach of ethics for a regulated profession;

(*h*) monitoring, inspection or exercise of a regulatory function by a public authority;

(*i*) protecting the data subject or the rights and freedoms of another natural person; or

(*j*) the enforcement of a civil law claim.

Part V—Duties of a Data Controller and Data Processor

Adherence to data protection principles

27. A data controller and data processor shall adhere to the principles relating to processing of personal data prescribed under Part III.

Technical and organizational measures

28. A data controller and data processor shall develop and implement appropriate technical and organizational measures to ensure that the processing of personal data complies with the provisions of this Act.

Record of personal data processing activities

29.—(1) A data controller and data processor shall maintain, in writing, a record of each personal data processing activity.

(2) The record referred to in subsection (1) shall contain—

(*a*) the name and contact details of the data controller or data processor and where applicable, a joint data controller, the representative of the data controller or data processor and the designated data protection officer;

(*b*) the purpose of processing the personal data;

(*c*) a description of the categories of data subjects and the categories of personal data;

(*d*) the categories of recipients to whom the personal data has been, or will be, disclosed;

(*e*) where possible, the envisaged time limits for the erasure of the different categories of the personal data;

(*f*) where possible, a general description of the technical and organizational measures implemented to adhere to this Act; and

(*g*) any other information as may be prescribed by the Authority.

(3) A data controller shall, on demand, make available to the Authority the record maintained under subsection (1).

Data protection impact assessment

30.—(1) Where the processing of personal data is likely to be of high risk to the rights and freedoms of a data subject by virtue of the nature of the data and the scope, context and purpose of the processing, a data controller shall, prior to the processing, carry out a data protection impact assessment.

(2) Notwithstanding the generality of subsection (1), a data controller shall conduct a data protection impact assessment—

(*a*) where the personal data will be processed using an automated processing system, including profiling;

(*b*) where sensitive personal data or personal data relating to a criminal offence or conviction will be processed on a large scale;

(*c*) where there will be systematic monitoring of a publicly accessible area on a large scale; or

(*d*) in any circumstance prescribed by the Authority, by a notice published in the *Gazette*.

(3) A data protection impact assessment shall contain—

(*a*) a systematic description of the envisaged personal data processing;

(*b*) the purpose of the processing of the personal data;

(*c*) where applicable, the legitimate interest pursued by the data controller, data processor or third party, as the case may be;

(*d*) an assessment of the necessity and proportionality of the processing of the personal data, in relation to the purpose of processing the data;

(*e*) an assessment of the risk to the rights and freedoms of the data subject;

(*f*) the measures envisaged to be put in place to address the risk, taking into account the rights, and legitimate interests of the data subject and any other natural person concerned; and

(*g*) any other information as may be prescribed by the Authority.

(4) A data controller shall submit the data impact assessment report to the Authority, prior to the processing of the personal data.

(5) A data controller shall, where there is a change in the risk represented in the data protection impact assessment report, carry out a review of the risk to assess if the processing of the personal data is being done in accordance with the data protection impact assessment.

(6) The Authority may by notice published in the *Gazette*, prescribe guidelines for carrying out a data protection impact assessment.

(7) The Minister may, by an order published in the *Gazette*, exempt a data controller or data processor from the obligation prescribed under subsection (1).

Joint data controllers

31.—(1) Where two or more data controllers jointly determine the purpose and means of processing personal data of a data subject, the data controllers shall be joint data controllers.

(2) Joint data controllers shall enter into a written agreement that clearly stipulates the role of each data controller and assign the duties under this Part to the joint data controllers.

(3) Joint data controllers shall provide a summary of the agreement entered into under subsection (2) to the data subject whose personal data is to be processed under the agreement.

(4) Joint data controllers shall be jointly and severally liable to the data subject whose personal data is processed under the agreement.

Regulation of the relationship between data controllers and data processors

32.—(1) A data controller and a data processor who intend to process personal data of a data subject shall enter into a written contract that sets out—

(*a*) the subject matter and duration of the processing of the data;

(*b*) the nature and purpose of the processing of the data;

(*c*) the type of data and categories of data subjects;

(*d*) the rights and duties of the data controller and data processor; and

(*e*) any other matter as may be prescribed by the Authority.

(2) A data processor shall not engage another data processor to process data covered by a contract entered into under subsection (1) without prior written authorization of the data controller.

(3) Where a data processor intends to engage another data processor or replace any other data processor engaged to process personal data of a data subject in accordance with subsection (1), the data processor shall inform the data controller of the intended addition or replacement of the other data processor.

(4) The data controller may object to any addition, or replacement, of a data processor communicated under subsection (3).

(5) The Authority may, for the purposes of this section, issue guidelines providing for any other matter regarding the relationship between a data controller and a data processor.

Designation of a data protection officer

33.—(1) A data controller and data processor shall, where—

(*a*) the data processing is carried out by a public authority;

(*b*) the core activities of the data controller or data processor consist of processing operations which, by virtue of their nature, scope and purposes, require regular and systematic monitoring of data subjects on a large scale; or

(*c*) the core activities of the data controller or data processor consist of processing, on a large scale, sensitive personal data, pursuant to section 16 or personal data relating to criminal offences and convictions pursuant to section 18,

designate a suitably qualified person as a data protection officer.

(2) For the purposes of this section, "public authority" shall not include a court of law.

Duties of a data protection officer

34. A data protection officer shall—

(*a*) advise a data controller or data processor on the obligations of the data controller or data processor under this Act;

(*b*) monitor compliance of the data controller or data processor with this Act and any data protection policy developed and implemented by the data controller or data processor;

(*c*) advise the data controller or data processor on data protection impact assessments; and

(*d*) act as the contact point for the Authority and the data controller or data processor, on compliance matters under this Act.

Part VI—Data Security

Security of personal data

35.—(1) A data controller and data processor shall, taking into account—

(*a*) the cost of technology;

(*b*) the nature, scope, context and purpose of processing personal data;

(*c*) the degree and likelihood of harm to a data subject that could result from the loss, disclosure or other misuse of personal data; and

(*d*) the retention period of personal data,

implement appropriate technical and organizational measures to ensure the security of personal data under the control or possession of the data controller or data processor.

(2) Notwithstanding the generality of subsection (1), a data controller and data processor shall implement the following measures to ensure the security of personal data—

(*a*) pseudonymization or any other method of de-identification of personal data;

(*b*) encryption of personal data;

(*c*) develop and implement procedures to restore availability and access to personal data in a timely manner in the event of a physical or technical incident;

(*d*) conduct periodic risk assessment of the data processing system and service including, without limitation, where the processing involves the transmission of personal data over an electronic communication network;

(*e*) conduct regular testing, assessment and evaluation of the effectiveness of the measures implemented under this section and section 30 against current and evolving risks; and

(*f*) carry out regular updates of the measures implemented under this section and introduce new measures to address any shortcomings in effectiveness identified and address evolving risks.

Notification of personal data breach

36.—(1) A data controller shall, in the case of a personal data breach, notify the Authority within seventy-two hours of becoming aware of the breach.

(2) The notification referred to in subsection (1) shall include—

(*a*) a description of the nature of the personal data breach;

(*b*) where possible, a description of the categories of personal data affected by the breach;

(*c*) where possible, the number of data subjects affected by the breach;

(*d*) a description of the likely consequences of the personal data breach;

(*e*) a description of the measures taken or proposed to be taken by the data controller to address the personal data breach; and

(*f*) the name and contact details of the data protection officer of the data controller.

(3) Where it is not practically possible for a data controller to provide the information referred to in subsection (2) within the period prescribed under subsection (1), the data controller shall provide the information as soon as the information becomes available.

(4) A data controller shall, with respect to each personal data breach, keep a record of the breach and the information prescribed under subsection (2).

(5) Where a personal data breach occurs while data is being processed by a data processor, the data processor shall notify the data controller of the breach, within seventy-two hours of the data processor becoming aware of the breach.

(6) The notification under subsection (5) shall contain the particulars prescribed under subsection (2).

Communication of personal data breach to data subjects

37.—(1) A data controller shall, where there is a personal data breach which is of high risk to rights and freedoms of a data subject, notify the data subject of the breach, within seventy-two hours of the data controller becoming aware of the breach.

(2) A data controller shall, in evaluating whether a personal data breach is likely to be of high risk to the rights and freedoms of a data subject, 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 personal data;

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

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

(3) The notification referred to in subsection (1) shall describe the nature of the personal data breach, the likely consequence of the breach and the measures taken or proposed to be taken by the data controller to address the breach.

(4) Where the notification referred to in subsection (1) involves a disproportionate effort or expense, the data controller shall make a public notification, in at least one newspaper of wide circulation in Malawi and any other mode of communication the data controller considers appropriate.

(5) Where the Authority is of the opinion that the measures taken by the data controller under this section are inadequate, the Authority may, at any time, make a public notification of the personal data breach, in at least one newspaper of wide circulation in Malawi or any other mode of communication the Authority considers appropriate.

Part VII—Cross-Border Transfers of Personal Data

Cross-border transfer of personal data

38.—(1) A data controller and data processor shall not transfer personal data from Malawi to another country or an international organization, unless—

(*a*) the recipient of the data is subject to—

(i) a law;

(ii) a binding corporate rule;

(iii) a personal data protection contractual clause;

(iv) code of conduct; or

(v) a certification mechanism,

that affords an adequate level of protection of personal data in accordance with section 39(2) and (3); or

(*b*) one of the conditions prescribed under section 39(4) applies.

(2) A data controller and data processor shall keep a record of the basis for the transfer of personal data from Malawi to another country or an international organization.

Adequacy of protection of personal data

39.—(1) The Authority shall, on application by a data controller or on its own initiative, assess whether an international organization

or a recipient of personal data outside Malawi provides adequate level of protection of personal data.

(2) The Authority shall, when carrying out an assessment for purposes of subsection (1), take into account—

(*a*) the availability of enforceable data subject rights and the availability of mechanisms for data subjects to enforce their rights through administrative or judicial processes;

(*b*) respect for the rule of law and human rights and freedoms by the country;

(*c*) the existence of a legally binding instrument between the Authority and the relevant public authority in the country, addressing elements of adequacy of data protection;

(*d*) the prevailing policy on access to personal data by a public authority in the country;

(*e*) the existence of an effective data protection law in the country;

(*f*) the existence of a functionally independent and competent data protection or similar supervisory authority with adequate enforcement powers; and

(g) international commitment and convention binding on the country, including its membership in a relevant multilateral or regional organization.

(3) The Authority may decide whether an international organization or a recipient of personal data outside Malawi provides an adequate level of protection of personal data based on comparable adequacy decision made by a competent data protection authority in another country.

(4) Where an international organization or a recipient of personal data outside Malawi does not provide an adequate level of protection of personal data in accordance with this section, a data controller or data processor shall not transfer personal data of a data subject to that international organization or that recipient, unless—

(*a*) the data subject has provided consent to the transfer of his or her personal data, upon being informed of the possible risk of the transfer;

(*b*) the processing of the data is necessary for the performance of a contract to which the data subject is a party or, at the request of the data subject, the implementation of a pre-contractual measure;

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

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

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

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

(5) Without prejudice to subsection (1), the Minister may, from time to time, by notice published in the *Gazette*, designate a country, region or specified sector within a country, or a standard personal data protection contractual clause as affording an adequate level of protection of personal data in accordance with this section.

Binding corporate rules, certification mechanisms, etc.

40. Where a data controller or data processor adopts binding corporate rules, code of conduct or certification mechanism, pursuant to this Act, the data controller or data processor shall submit the adopted corporate rules, code of conduct or certification mechanism to the Authority.

Part VIII—Registration of Data Controllers of Significant Importance and Data Processors of Significant Importance

Registration of data controllers of significant importance and data processors of significant importance

41.—(1) A data controller or data processor shall not process personal data as a data controller of significant importance and a data processor of significant importance, unless the data controller or data processor is registered as a data controller of significant importance or a data processor of significant importance, as the case may be, under this Part.

(2) A data controller or data processor who intends to process personal data as a data controller of significant importance or a data processor of significant importance shall submit an application for registration, in the prescribed form, to the Authority and the application shall be accompanied by the prescribed fee.

(3) The Authority shall, within fourteen days of receiving an application under subsection (2)—

Complaints

(*a*) register the data controller or data processor as a data controller of significant importance or data processor of significant importance, as the case may be; or

(*b*) refuse to register the data controller or data processor as a data controller of significant importance or data processor of

significant importance and provide reasons for the refusal, in writing, to the applicant.

(4) Where the Authority registers a data controller or data processor as a data controller of significant importance or data processor of significant importance in accordance with subsection (3)(*a*), the Authority shall issue a registration certificate in the prescribed form to the data controller or data processor.

(5) The Authority may impose such terms and conditions on the registration as it determines appropriate.

(6) A registered data controller of significant importance or data processor of significant importance shall, where there is a change to the information provided to the Authority during registration, notify the Authority of the change, in writing, within ninety days of the change.

(7) The Authority shall keep and maintain, in the prescribed form, a register of data controllers of significant importance and data processors of significant importance.

Suspension or cancellation of registration

42.—(1) The Authority may suspend or cancel the registration of a data controller of significant importance or data processor of significant importance where the Authority is satisfied that—

(*a*) the data controller of significant importance or data processor of significant importance—

(i) has not complied with any provision of this Act or any term or condition imposed on the registration; or

(ii) made a misleading or false representation at the time of registration; or

(*b*) there is any other reasonable ground to suspend or cancel the registration.

(2) The Authority shall not suspend or cancel the registration of a data controller of significant importance or data processor of significant importance under subsection (1), unless the data controller of significant importance or data processor of significant importance has been given an opportunity to show cause why the registration should not be suspended or cancelled.

Exemptions

43. The Minister may, by order published in the *Gazette*, exempt a class of data controllers of significant importance or data processors of significant importance from the registration requirement under this Part.

Part IX—Complaints

Complaints

44.—(1) A data subject who is aggrieved by any action or inaction of a data controller or data processor may lodge a complaint, in writing, with the Authority.

(2) Where a parent or legal guardian of a data subject who is a child or any other natural person lacking legal capacity believes that a right of the data subject under this Act has been violated, the parent or legal guardian may lodge a complaint, in writing, with the Authority.

(3) The Authority shall investigate any complaint received under subsection (1) or (2) if—

(*a*) the complaint is lodged within ninety days of the action or inaction on which the complaint is based; and

(*b*) the complaint is not frivolous or vexatious.

(4) The Authority may, on its own initiative, investigate any matter where the Authority has reasonable grounds to believe that a data controller or data processor has contravened, or is likely to contravene, this Act.

(5) The Authority may, for purposes of an investigation under this section, order any person to—

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

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

(*c*) furnish a statement, in writing, made under oath setting out any information which may be required.

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

(7) The Authority shall, within thirty days of completing any investigation conducted under this section, communicate the results of the investigation to—

(*a*) where the investigation was based on a complaint received by the Authority, the person who lodged the complaint and the

data controller or data processor, as the case may be, under investigation; or

(*b*) where the investigation was done on the Authority's own initiative, the data controller or data processor, as the case may be, under investigation.

Compliance orders

45.—(1) Where upon conclusion of an investigation under section 44, the Authority is satisfied that a data controller or data processor has contravened or is likely to contravene this Act, the Authority shall issue an appropriate compliance order to the data controller or data processor.

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

(*a*) an order requiring the data controller or data processor to comply with a specified provision of this Act;

(*b*) a cease and desist order requiring the data controller or data processor to stop or refrain from doing an act which is in contravention of this Act;

(*c*) an order requiring the data controller or data processor to pay compensation to a data subject affected by the action or inaction of the data controller or data processor;

(*d*) an order requiring the data controller or data processor to account for the profits made out of the contravention;

(*e*) an order requiring the data controller or data processor to pay an administrative penalty not exceeding K20,000,000; or

(*f*) any other order as the Authority may consider just and appropriate.

(3) A compliance order issued under this section shall be in writing and shall specify—

(*a*) the provision of the Act that the data controller or data processor has contravened or is likely to contravene;

(*b*) the specific measures to be taken by the data controller or data processor to avoid, remedy or eliminate the situation which has resulted, or is likely to result, in the contravention;

(*c*) a period within which any action specified in the order is to be implemented; and

(*d*) the right of the data controller or data processor to seek review of the decision by the High Court and the period within which to seek the review.

(4) A data controller or data processor who fails to comply with a compliance order other than an order to pay compensation or an

administrative penalty or an order to make good of profits, issued pursuant to this section commits an offence and shall, upon conviction, be liable to—

(*a*) in the case of a natural person, a fine of K10,000,000 and to imprisonment for two years; or

(*b*) in the case of a legal person, a fine of K50,000,000.

(5) Where pursuant to this section, the Authority imposes an order to pay compensation or make good of profits or pay an administrative penalty on a data controller or data processor and the data controller or data processor fails to pay the compensation or penalty of make good of the profits within thirty days from the date the data controller or data processor receives the decision, the Authority may recover the compensation profits or penalty as a civil debt due to the awardee of the compensation or the Authority, as the case may be.

Part X—Miscellaneous

Appeal against decisions of the Authority

46.—(1) A person aggrieved by a decision of the Authority under this Act may, within thirty days of receiving the decision, apply to the High Court for review of the decision.

(2) The High Court shall, upon hearing a matter brought pursuant to subsection (1)—

(*a*) confirm, vary or set aside the decision; or

(*b*) make any other order as the court considers fair and just.

Civil remedies

47. Notwithstanding sections 44 and 45, a data subject who suffers injury, loss or harm, as a result of a contravention of this Act by a data controller or data processor, may commence legal action for a civil remedy against the data controller or data processor concerned.

Obstruction, interference with the Authority

48. A person who obstructs or interferes with the Authority, an officer of the Authority or any person authorized by the Authority to carry out any function under this Act in the performance of any function under this Act, commits an offence and shall, upon conviction, be liable to a fine of K10,000,000 and to imprisonment for two years.

Breach of confidentiality

49. A person who—

(*a*) being a member of the Authority, an employee of the Authority or a person authorized to perform any function under this Act, publishes or communicates to any other person without lawful authority any information acquired by that person in the course of duty; or

(*b*) is in possession of any information which to the knowledge of the person was obtained in contravention of this Act, publishes or communicates that information without lawful authority to any other person,

commits an offence and shall, upon conviction, be liable to a fine of K20,000,000 and to imprisonment for five years.

Offences committed by legal persons, firms, etc.

50.—(1) Where a legal person is convicted of an offence under this Act, every natural person who—

(*a*) is a director of, or is otherwise concerned with the management of, the legal person; and

(*b*) knowingly authorized or permitted the act or omission constituting the offence,

commits the same offence which the legal person is guilty of, and may be proceeded against and be sentenced in the same manner as any other natural person.

(2) A natural person who is a partner in a firm shall be jointly and severally liable for any act or omission of the other partner in the firm in so far as the act or omission relates to the firm.

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

Vicarious liability

51. A data controller and data processor shall be vicariously liable for any act or omission of an agent, employee or other person authorized by the data controller or data processor to perform any function regulated under this Act, in so far as the act or omission relates to an operation of the data controller or data processor.

Regulations

52.—(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 make provision for—

(*a*) forms, certificates and registers required under this Act;

(*b*) fees payable under this Act;

(*c*) the procedure for receiving and handling complaints;

(*d*) the criteria for classifying data controllers of

significant importance and data processors of significant importance;

(*e*) the form of binding corporate rules, codes of conduct or certification mechanisms; and

(*f*) any matter required to be prescribed under this Act.

Cap. 1:01

(3) Notwithstanding the provisions of section 21(*e*) of the General Interpretation Act, the regulations made under subsection (1), may provide for offences the contravention of which may attract a penalty of a fine of K5,000,000 and imprisonment for twelve months.

Transitional provision

53. A data controller or a data processor who is domiciled, ordinarily resident, or ordinarily operates in Malawi and—

(*a*) is not a data controller of significant importance or data processor of significant importance shall be exempt from compliance with this Act, for a period of twenty-four months from the date the Act comes into operation; or

(*b*) is a data controller of significant importance or data processor of significant importance shall, within six months from the date the Act comes into operation, comply with the requirements prescribed under this Act.

Passed in Parliament this seventh day of December, two thousand and twenty-three.

FIONA KALEMBA
Clerk of Parliament