THE DATA PROTECTION ACT 2017

Act No. 20 of 2017

I assent

BIBI AMEENAH FIRDAUS GURIB-FAKIM
22 December 2017 *President of the Republic*

ARRANGEMENT OF SECTIONS

Section

An Act

To provide for new legislation to strengthen the control and personal autonomy of data subjects over their personal data, in line with current relevant international standards, and for matters related thereto

ENACTED by the Parliament of Mauritius, as follows –

PART I – PRELIMINARY

1. Short title

This Act may be cited as the Data Protection Act 2017.

2. Interpretation

In this Act –

"authorised officer" means an officer to whom the Commissioner has delegated his powers under section 13;

"biometric data" means any personal data relating to the physical, physiological or behavioural characteristics of an individual which allow his unique identification, including facial images or dactyloscopic data;

"collect" does not include receive unsolicited information;

"Commissioner" means the Data Protection Commissioner referred to in section 4;

"consent" means any freely given specific, informed and unambiguous indication of the wishes of a data subject, either by a statement or a clear affirmative action, by which he signifies his agreement to personal data relating to him being processed;

"controller" means a person who or public body which, alone or jointly with others, determines the purposes and means of the processing of personal data and has decision making power with respect to the processing;

"data subject" means an identified or identifiable individual, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual;

"document" includes –

(a) a disc, tape or other device in which information other than visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced from the disc, tape or other device; and

(b) a film, tape or other device in which visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced from the film, tape or other device;

"encryption" means the process of transforming data into coded form;

"filing system" means a structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

"genetic data" means personal data relating to the general characteristics of an individual which are inherited or acquired and which provide unique information about the physiology or health of the individual and which result, in particular, from an analysis of a biological sample from the individual in question;

"physical or mental health", in relation to personal data, includes information on the provision of health care services to the individual, which reveals his health status;

"individual" means a living individual;

"information and communication network" –

(a) means a network for the transmission of messages; and

(b) includes a telecommunication network;

"Minister" means the Minister to whom responsibility for the subject of data protection is assigned;

"network" means a communication transmission system that provides interconnection among a number of local and remote devices;

"Office" means the Data Protection Office referred to in section 4;

"personal data" means any information relating to a data subject;

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

"proceedings" –

(a) means any proceedings conducted by or under the supervision of a Judge or Magistrate; and

(b) may include –

(i) an inquiry or investigation into an offence; and

(ii) disciplinary proceedings;

"processor" means a person who, or public body which, processes personal data on behalf of a controller;

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

"profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

"pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information and the additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable individual;

"recipient" means a person to whom, or a public body to which, personal data are disclosed, whether a third party or not;

"register" means the register referred to in section 20;

"registration certificate" means the registration certificate referred to in section 16 (2);

"restriction of processing" means the marking of stored personal data with the aim of limiting their processing in the future;

"special categories of personal data", in relation to a data subject, means personal data pertaining to –

(a) his racial or ethnic origin;

(b) his political opinion or adherence;

(c) his religious or philosophical beliefs;

(d) his membership of a trade union;

(e) his physical or mental health or condition;

(f) his sexual orientation, practices or preferences;

(g) his genetic data or biometric data uniquely identifying him;

(h) the commission or alleged commission of an offence by him;

(i) any proceedings for an offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any Court in the proceedings; or

(j) such other personal data as the Commissioner may determine to be sensitive personal data;

"telecommunication network" means a system, or a series of systems, operating within such boundaries as may be prescribed, for the transmission or reception of messages by means of guided or unguided electro magnetic energy or both;

"third party" means a person or public body other than a data subject, a controller, a processor or a person who, under the direct authority of a controller or processor, who or which is authorised to process personal data;

"traffic data" means any data relating to a communication by means of a computer system and generated by the system that form part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service;

"Tribunal" means the ICT Appeal Tribunal set up under section 35 of the Information and Communication Technologies Act.

3. Application of Act

(1) This Act shall bind the State.

(2) For the purposes of this Act, each Ministry or Government department shall be treated as separate from any other Ministry or Government department.

(3) This Act shall apply to the processing of personal data, wholly or partly, by automated means and to any processing otherwise than by automated means where the personal data form part of a filing system or are intended to form part of a filing system.

(4) This Act shall not apply to –

(a) the exchange of information between Ministries, Government departments and public sector agencies where such exchange is required on a need-to-know basis;

(b) the processing of personal data by an individual in the course of a purely personal or household activity.

(5) Subject to section 44, this Act shall apply to a controller or processor who –

(a) is established in Mauritius and processes personal data in the context of that establishment; and

(b) is not established in Mauritius but uses equipment in Mauritius for processing personal data, other than for the purpose of transit through Mauritius.

(6) Every controller or processor referred to in subsection (5)(b) shall nominate a representative established in Mauritius.

(7) For the purpose of subsection (5)(a), any person who –

(a) is ordinarily resident in Mauritius; or

(b) carries out data processing operations through an office, branch or agency in Mauritius,

shall be treated as being established in Mauritius.

PART II – DATA PROTECTION OFFICE

Sub-Part A – Establishment of Data Protection Office

4. Establishment of Office

(1) There shall, for the purposes of this Act, be a public office to be known as the Data Protection Office.

(2) In the discharge of its functions under this Act, the Office shall act with complete independence and impartiality and shall not be subject to the control or direction of any other person or authority.

(3) The head of the Office, who shall be known as the Data Protection Commissioner, shall be a barrister of not less than 5 years' standing.

(4) The Commissioner shall be assisted by such public officers as may be necessary.

(5) Every public officer referred to in subsection (4) shall be under the administrative control of the Commissioner.

Sub-Part B – Functions and Powers of Commissioner

5. Functions of Commissioner

The Commissioner shall –

(a) ensure compliance with this Act and any regulations made under it;

(b) issue or approve such Codes of Practice or Guidelines for the purposes of this Act as he thinks fit;

(c) maintain a register of controllers and processors;

(d) exercise control on all data processing operations, either of his own motion or at the request of a data subject, and verify whether the processing of data is done in accordance with this Act;

(e) promote self-regulation among controllers and processors;

(f) investigate any complaint or information which gives rise to a suspicion that an offence may have been, is being or is about to be, committed under this Act;

(g) take such measures as may be necessary to bring the provisions of this Act to the knowledge of the general public;

(h) undertake research into, and monitor developments in, data processing, and ensure that there is no significant risk or adverse effect of any developments on the privacy of individuals;

(i) examine any proposal for automated decision making or data linkage that may involve an interference with, or may otherwise have an adverse effect, on the privacy of individuals and ensure that any adverse effect of the proposal on the privacy of individuals is minimised;

(j) cooperate with supervisory authorities of other countries, to the extent necessary for the performance of his duties under this Act, in particular by exchanging relevant information in accordance with any other enactment; and

(k) do anything incidental or conducive to the attainment of the objects of and to the better performance of his duties and functions under, this Act.

6. Investigation of complaints

(1) Where a complaint is made to the Commissioner that this Act or any regulations made under it, has or have been, is or are being, or is or are about to be, contravened, the Commissioner shall –

(a) investigate into the complaint or cause it to be investigated by an authorised officer, unless he is of the opinion that the complaint is frivolous or vexatious; and

(b) where he is unable to arrange, within a reasonable time, for the amicable resolution by the parties concerned of the complaint, notify, in writing, the individual who made the complaint of his decision in relation to it so that the individual may, where he considers that he is aggrieved by the decision, appeal against it under section 51.

(2) (a) The Commissioner may, for the purpose of the investigation of a complaint, order any person to –

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

(ii) produce such book, document, record or article as may be required with respect to any matter relevant to the investigation, which he is not prevented by any other enactment from disclosing; or

(iii) furnish a statement in writing made under oath or on affirmation setting out all information which may be required under the notice.

(b) Every order made under paragraph (a) shall be in writing and signed by the Commissioner or an authorised officer.

(3) A person on whom an order under subsection (2) has been served shall –

(a) comply with the order;

(b) attend before the Commissioner in accordance with the terms of the order or on such other days as he may be directed to attend; and

(c) answer questions and furnish all information, documents, records or statements, including certified copies thereof, as ordered.

(4) (a) The Commissioner may take copies or extracts from any document produced under subsection (2) and may require the person producing it to give any necessary explanation relating to such document.

(b) Where material to which an investigation relates consists of information stored in a computer, disc or cassette, or on microfilm, or preserved by any mechanical or electronic device, the request from the Commissioner may require the person named therein to produce or give access to it in a form in which it can be taken away and in which it is visible and legible.

(5) Any person who, without lawful or reasonable excuse, fails to attend a hearing or to produce a document or other material when required to do so under subsection (4) shall commit an offence and shall, on conviction, be liable to a fine not exceeding 50, 000 rupees and to imprisonment for a term not exceeding 2 years.

(6) Subject to this section, the Commissioner shall regulate the handling of complaints, investigations and conduct of hearings in such manner as he may determine.

(7) No person shall be required under this section to answer any question or to give any evidence tending to incriminate him.

7. Power to require information

(1) Subject to section 26 of the Bank of Mauritius Act, section 64 of the Banking Act, section 83 of the Financial Services Act, section 30 of the Financial Intelligence and Anti-Money Laundering Act and section 81 of the Prevention of Corruption Act –

(a) the Commissioner may, by written notice served on a person, request from that person such information as is necessary or expedient for the discharge of his functions and the exercise of his powers under this Act; and

(b) where the information requested by the Commissioner is stored in a computer, disc or cassette, or on microfilm, or preserved by any mechanical or electronic device, the person named in the notice shall produce or give access to the information in a form in which it can be taken away and in which it is visible and legible.

(2) Any person who, without reasonable excuse, fails or refuses to comply with a requirement specified in a notice, or who furnishes to the Commissioner any information which he knows to be false or misleading in a material particular, shall commit an offence and shall, on conviction, be liable to a fine not exceeding 50, 000 rupees and to imprisonment for a term not exceeding 2 years.

8. Preservation Order

(1) The Commissioner may apply to a Judge in Chambers for a Preservation Order for the expeditious preservation of data, including traffic data, where he has reasonable ground to believe that the data are vulnerable to loss or modification.

(2) Where the Judge is satisfied that a Preservation Order may be made under subsection (1), he shall issue the Preservation Order specifying a period which shall not be more than 90 days during which the order shall remain in force.

(3) The Judge may, on application made by the Commissioner, extend the period specified in subsection (2) for such period as he thinks fit.

9. Enforcement notice

(1) Where the Commissioner is of the opinion that a controller or a processor has contravened, is contravening or is about to contravene this Act, the Commissioner may serve an enforcement notice on him requiring him to take such steps within such period as may be specified in the notice.

(2) Notwithstanding subsection (1), where the Commissioner is of the opinion that a person has committed an offence under this Act, he may investigate the matter or cause it to be investigated by an authorised officer.

(3) An enforcement notice served under subsection (1) shall –

(a) specify the provision of this Act which has been, is being or is likely to be, contravened;

(b) specify the measures that shall be taken to remedy or eliminate the situation which makes it likely that a contravention will arise;

(c) specify a period which shall not be less than 21 days within which those measures shall be implemented; and

(d) state that a right of appeal is available under section 51.

(4) On complying with an enforcement notice, the controller or processor, as the case may be, shall, not later than 21 days after compliance, notify –

(a) the data subject concerned; and

(b) where such compliance materially modifies the data concerned, any person to whom the data was disclosed during the period beginning 12 months before the date of the service of the notice and ending immediately before compliance,

of any amendment.

(5) Where the Commissioner considers that any provision of the enforcement notice may not be complied with to ensure compliance with this Act, he may vary the notice and, where he does so, he shall give written notice to the person on whom the notice was served.

(6) Any person who, without reasonable excuse, fails or refuses to comply with an enforcement notice shall commit an offence and shall, on conviction, be liable to a fine not exceeding 50, 000 rupees and to imprisonment for a term not exceeding 2 years.

10. Power to seek assistance

(1) For the purpose of gathering information or for the proper conduct of any investigation under this Act, the Commissioner may seek the assistance of such person or authority as he thinks fit and that person or authority may do such things as are reasonably necessary to assist the Commissioner in the discharge of his functions.

(2) Any person assisting the Commissioner pursuant to subsection (1) shall, for the purpose of section 49, be considered to be an authorised officer.

Sub-Part C – Powers of Authorised Officers

11. Power of entry and search

(1) Subject to this section, an authorised officer may enter and search any premises for the purpose of discharging any function or exercising any power under this Act.

(2) No authorised officer shall enter or search any premises unless he shows to the owner or occupier a warrant issued by a Magistrate for the purpose referred to in subsection (1).

(3) A Magistrate may, on being satisfied on an information upon oath that entry and search into any premises are necessary to enable the authorised officer to discharge any of his functions or exercise any of his powers under this Act, issue a warrant authorising the authorised officer to enter and search the premises.

(4) A warrant issued under subsection (3) shall be valid for the period stated in the warrant and may be subject to such condition as the Magistrate may specify.

(5) Subject to section 26 of the Bank of Mauritius Act, section 64 of the Banking Act, section 83 of the Financial Services Act, section 30 of the Financial Intelligence and Anti-Money Laundering Act and section 81 of the Prevention of Corruption Act, an authorised officer may, on entering any premises –

(a) request the owner or occupier to produce any document, record or data;

(b) examine any such document, record or data and take copies or extracts from them;

(c) request the owner of the premises entered into, any person employed by him, or any other person on the premises, to give to the authorised officer all reasonable assistance and to answer all reasonable questions, orally or in writing.

(6) Where any information requested by the authorised officer is stored in a computer, disc or cassette, or on microfilm, or preserved by any mechanical or electronic device, the person to whom the request is made shall be deemed to be required to produce or give access to it in a form in which it can be taken away and in which it is visible and legible.

(7) For the purpose of discharging his functions under this section, the authorised officer may be accompanied by such person as the Commissioner may determine.

12. Obstruction of Commissioner or authorised officer

Any person who, in relation to the exercise of a power conferred by section 11 –

(a) obstructs or impedes the Commissioner or an authorised officer in the exercise of such power;

(b) fails to provide assistance or information requested by the Commissioner or authorised officer;

(c) refuses to allow the Commissioner or an authorised officer to enter any premises or to take any person with him in the exercise of his functions;

(d) gives to the Commissioner or an authorised officer any information which is false or misleading in a material particular,

shall commit an offence and shall, on conviction, be liable to a fine not exceeding 50, 000 rupees and to imprisonment for a term not exceeding 2 years.

Sub-Part D – Delegation of Power

13. Delegation of power by Commissioner

The Commissioner may delegate any investigating or enforcement power conferred on him by this Act to an officer of the Office or to a police officer designated for that purpose by the Commissioner of Police.

PART III – REGISTRATION OF CONTROLLERS AND PROCESSORS

14. Controller and Processor

Subject to section 44, no person shall act as controller or processor unless he or it is registered with the Commissioner.

15. Application for registration

(1) Every person who intends to act as a controller or processor shall apply to the Commissioner, in such form as the Commissioner may approve, to be registered as controller or processor.

(2) Every application under subsection (1) shall be accompanied by the following particulars regarding the applicant –

(a) name and address;

(b) if he or it has nominated a representative for the purposes of this Act, the name and address of the representative;

(c) a description of the personal data to be processed by the controller or processor, and of the category of data subjects, to which the personal data relate;

(d) a statement as to whether or not he or it holds, or is likely to hold, special categories of personal data;

(e) a description of the purpose for which the personal data are to be processed;

(f) a description of any recipient to whom the controller intends or may wish to disclose the personal data;

(g) the name, or a description of, any country to which the proposed controller intends or may wish, directly or indirectly, to transfer the data; and

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

(3) Any controller or processor who knowingly supplies any information under subsection (1) which is false or misleading in a material particular shall commit an offence and shall, on conviction, be liable to a fine not exceeding 100, 000 rupees and to imprisonment for a term not exceeding 5 years.

16. Issue of registration certificate

(1) Where the Commissioner considers that an applicant meets the criteria to be registered as a controller or processor, as the case may be, he shall grant the application.

(2) Where the Commissioner grants an application for registration as a controller or processor, he shall, on such terms and conditions as he may determine, register the applicant as a controller or processor, as the case may be, and issue the applicant, on payment of such fee as may be prescribed, with a registration certificate in such form and manner as the Commissioner may determine.

(3) A registration certificate issued under subsection (2) shall be valid for a period of 3 years.

17. Change in particulars

(1) Where, following the grant of an application, there is a change in any of the particulars referred to in section 15(2), the controller or processor, shall, within 14 days of the date of the change, notify the Commissioner in writing of the nature and date of the change.

(2) On receipt of a notification under subsection (1), the Commissioner, on being satisfied that there is a change in particulars, shall amend the appropriate entry in the register.

(3) Any controller or processor who fails to comply with subsection (1) shall commit an offence and shall, on conviction, be liable to a fine not exceeding 50, 000 rupees.

18. Renewal of registration certificate

(1) The holder of a registration certificate may apply for the renewal of the certificate not later than 3 months before the date of its expiry.

(2) Where the Commissioner grants an application under subsection (1), he shall, on such terms and conditions as he may determine and on payment of such fee as may be prescribed, issue a new registration certificate.

19. Cancellation or variation of terms and conditions of registration certificate

(1) Subject to this section, the Commissioner may cancel a registration certificate or vary its terms and conditions where –

(a) any information given to him by the applicant is false or misleading in any material particular;

(b) the holder of the registration certificate fails, without lawful excuse, to comply with –

(i) any requirement of this Act; or

(ii) any term or condition specified in the certificate.

(2) The Commissioner shall, before cancelling or varying the terms and conditions of a registration certificate, require, by notice in writing, the holder of the certificate to show cause, within 14 days of the notice, why the registration certificate should not be cancelled or its terms and conditions should not be varied.

20. Register of controllers and processors

(1) There shall be a register of controllers and processors to be known as the Data Protection Register, which shall be kept and maintained by the Commissioner in such form and manner as he may determine.

(2) The Commissioner may, at any time, at the request of a controller or processor, in respect of which there is an entry in the register and which has ceased to exist, remove its details from the register.

(3) (a) The register shall, at all reasonable times, be available for inspection by any person free of charge.

(b) Any person may, on payment of such fee as may be prescribed, obtain from the Commissioner a certified copy of, or of an extract from, any entry in the register.

PART IV – OBLIGATIONS ON CONTROLLERS AND PROCESSORS

21. Principles relating to processing of personal data

Every controller or processor shall ensure that personal data are –

(a) processed lawfully, fairly and in a transparent manner in relation to any data subject;

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

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data are erased or rectified without delay;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and

(f) processed in accordance with the rights of data subjects.

22. Duties of controller

(1) Every controller shall adopt policies and implement appropriate technical and organisational measures so as to ensure and be able to demonstrate that the processing of personal data is performed in accordance with this Act.

(2) The measures referred to in subsection (1) shall include –

(a) implementing appropriate data security and organisational measures in accordance with section 31;

(b) keeping a record of all processing operations in accordance with section 33;

(c) performing a data protection impact assessment in accordance with section 34;

(d) complying with the requirements for prior authorisation from, or consultation with the Commissioner pursuant to section 35; and

(e) designating an officer responsible for data protection compliance issues.

(3) Every controller shall implement such policies and mechanisms as may be required to ensure verification of the effectiveness of the measures referred to in this section.

23. Collection of personal data

(1) Subject to section 44, a controller shall not collect personal data unless –

(a) it is done for a lawful purpose connected with a function or activity of the controller; and

(b) the collection of the data is necessary for that purpose.

(2) Subject to subsection (3), where a controller collects personal data directly from a data subject, the controller shall, at the time of collecting the personal data, ensure that the data subject concerned is informed of –

(a) the identity and contact details of the controller and, where applicable, its representative and any data protection officer;

(b) the purpose for which the data are being collected;

(c) the intended recipients of the data;

(d) whether or not the supply of the data by that data subject is voluntary or mandatory;

(e) the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(f) the existence of the right to request from the controller access to and rectification, restriction or erasure of personal data concerning the data subject or to object to the processing;

(g) the existence of automated decision making, including profiling, and information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;

(h) the period for which the personal data shall be stored;

(i) the right to lodge a complaint with the Commissioner;

(j) where applicable, that the controller intends to transfer personal data to another country and on the level of suitable protection afforded by that country; and

(k) any further information necessary to guarantee fair processing in respect of the data subject's personal data, having regard to the specific circumstances in which the data are collected.

(3) A controller shall not be required to comply with subsection (2) where –

(a) the data subject already has the information referred to in subsections (1) and (2); or

(b) the data are not collected from the data subject and –

(i) the provision of such information proves impossible or would involve a disproportionate effort; or

(ii) the recording or disclosure of the data is laid down by law.

(4) Where data are not collected directly from the data subject concerned, the controller or any person acting on his or its behalf shall ensure that the data subject is informed of the matters specified in subsection (2).

24. Conditions for consent

(1) The controller shall bear the burden of proof for establishing a data subject's consent to the processing of his personal data for a specified purpose.

(2) The data subject shall have the right to withdraw his consent at any time.

(3) In determining whether consent was freely given, account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

25. Notification of personal data breach

(1) (a) In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Commissioner.

(b) Where the controller fails to notify the personal data breach within the time limit specified in paragraph (a), he shall provide the Commissioner with the reasons for the delay.

(2) Where a processor becomes aware of a personal data breach, he shall notify the controller without any undue delay.

(3) The notification referred to in subsection (1) shall –

(a) describe the nature of the personal data breach, including where possible, the categories and approximate number of data subjects and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of any appropriate data protection officer or other contact point where more information may be obtained; and

(c) recommend measures to address the personal data breach, including, where appropriate, measures to mitigate the possible adverse effects of the breach.

(4) The controller shall specify the facts relating to the personal data breach, its effects and the remedial action taken so as to enable the Commissioner to verify compliance with this section.

26. Communication of personal data breach to data subject

(1) Subject to subsection (3), where a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject, the controller shall, after the notification referred to in section 25, communicate the personal data breach to the data subject without undue delay.

(2) The communication to the data subject shall describe in clear language the nature of the personal data breach and set out the information and the recommendations provided for in section 25.

(3) The communication of a personal data breach to the data subject shall not be required where –

(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the breach, in particular, those that render the data unintelligible to any person who is not authorised to access it, such as encryption;

(b) the controller has taken subsequent measures to ensure that the high risk to the rights and freedoms of the data subject referred to in subsection (1) is no longer likely to materialise; or

(c) it would involve disproportionate effort and the controller has made a public communication or similar measure whereby data subject is informed in an equally effective manner.

(4) Where the controller has not already communicated the personal data breach to the data subject, the Commissioner may, after having considered the likelihood of the personal data breach resulting in a high risk, require it to do so.

27. Duty to destroy personal data

(1) Where the purpose for keeping personal data has lapsed, every controller shall –

(a) destroy the data as soon as is reasonably practicable; and

(b) notify any processor holding the data.

(2) Any processor who receives a notification under subsection (1)(b) shall, as soon as is reasonably practicable, destroy the data specified by the controller.

28. Lawful processing

(1) No person shall process personal data unless –

(a) the data subject consents to the processing for one or more specified purposes;

(b) the processing is necessary –

(i) for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;

(ii) for compliance with any legal obligation to which the controller is subject;

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

(iv) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(v) the performance of any task carried out by a public authority;

(vi) the exercise, by any person in the public interest, of any other functions of a public nature;

(vii) for the legitimate interests pursued by the controller or by a third party to whom the data are disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or

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

(2) Any person who contravenes subsection (1) shall commit an offence and shall, on conviction, be liable to a fine not exceeding 100, 000 rupees and to imprisonment for a term not exceeding 5 years.

29. Special categories of personal data

(1) Special categories of personal data shall not be processed unless –

(a) section 28 applies to the processing; and

(b) 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 political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(c) the processing relates to personal data which are manifestly made public by the data subject; or

(d) the processing is necessary for –

(i) the establishment, exercise or defence of a legal claim;

(ii) the purpose of preventive or occupational medicine, for the assessment of the working capacity of an employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services or pursuant to a contract with a health professional and subject to the conditions and safeguards referred to in subsection (2);

(iii) the purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject; or

(iv) protecting the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent.

(2) The personal data referred to in subsection (1) may be processed for the purposes referred to in subsection (1)(d)(ii) where the data are processed by or under the responsibility of a professional or other person subject to the obligation of professional secrecy under any enactment.

(3) Any person who contravenes subsection (1) shall commit an offence and shall, on conviction, be liable to a fine not exceeding 100, 000 rupees and to imprisonment for a term not exceeding 5 years.

30. Personal data of child

(1) No person shall process the personal data of a child below the age of 16 years unless consent is given by the child's parent or guardian.

(2) Where the personal data of a child below the age of 16 years is involved, a controller shall make every reasonable effort to verify that consent has been given or authorised, taking into account available technology.

31. Security of processing

(1) A controller or processor shall, at the time of the determination of the means for processing and at the time of the processing –

(a) implement appropriate security and organisational measures for –

(i) the prevention of unauthorised access to;

(ii) the alteration of;

(iii) the disclosure of;

(iv) the accidental loss of; and

(v) the destruction of,

the data in his control; and

(b) ensure that the measures provide a level of security appropriate for –

(i) the harm that might result from –

(A) the unauthorised access to;

(B) the alteration of;

(C) the disclosure of;

(D) the destruction of,

the data and its accidental loss; and

(ii) the nature of the data concerned.

(2) (a) The measures referred to in subsection (1) shall include –

(i) the pseudonymisation and encryption of personal data;

(ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

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

(iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

(b) The Office may lay down technical standards for the requirements specified in paragraph (a).

(3) In determining the appropriate security measures referred to in subsection (1), in particular, where the processing involves the transmission of data over an information and communication network, a controller shall have regard to –

(a) the state of technological development available;

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

(c) the special risks that exist in the processing of the data; and

(d) the nature of the data being processed.

(4) Where a controller is using the services of a processor –

(a) he or it shall choose a processor providing sufficient guarantees in respect of security and organisational measures for the purpose of complying with subsection (1); and

(b) the controller and the processor shall enter into a written contract which shall provide that –

(i) the processor shall act only on instructions received from the controller; and

(ii) the processor shall be bound by obligations devolving on the controller under subsection (1).

(5) Where a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing.

(6) Every controller or processor shall take all reasonable steps to ensure that any person employed by him or it is aware of, and complies with, the relevant security measures.

32. Prior security check

(1) Where the Commissioner is of the opinion that the processing or transfer of data by a controller or processor may entail a specific risk to the privacy rights of data subjects, he may inspect and assess the security measures taken under section 31 prior to the beginning of the processing or transfer.

(2) The Commissioner may, at any reasonable time during working hours, carry out further inspection and assessment of the security measures imposed on a controller or processor under section 31.

33. Record of processing operations

(1) Every controller or processor shall maintain a record of all processing operations under his or its responsibility.

(2) The record shall set out –

(a) the name and contact details of the controller or processor, and, where applicable, his or its representative and any data protection officer;

(b) the purpose of the processing;

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

(d) a description of the categories of recipients to whom personal data have been or will be disclosed, including recipients in other countries;

(e) any transfers of data to another country, and, in the case of a transfer referred to in section 36, the suitable safeguards;

(f) where possible, the envisaged time limits for the erasure of the different categories of data; and

(g) the description of the mechanisms referred to in section 22 (3).

(3) The controller or processor shall, on request, make the record available to the Office.

PART V – PROCESSING OPERATIONS LIKELY TO PRESENT RISK

34. Data protection impact assessment

(1) Where processing operations are likely to result in a high risk to the rights and freedoms of data subjects by virtue of their nature,

scope, context and purposes, every controller or processor shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

(2) The processing operations referred to in subsection (1) are –

(a) a systematic and extensive evaluation of personal aspects relating to individuals which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the individual or significantly affect the individual;

(b) processing on a large scale of special categories of data referred to in section 29;

(c) a systematic monitoring of a publicly accessible area on a large scale;

(d) any other processing operations for which consultation with the Office is required.

(3) An assessment shall include –

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller or processor;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

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

(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.

(4) Where appropriate, the controller or processor shall seek the views of data subjects on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.

35. Prior authorisation and consultation

(1) Every controller or processor shall obtain authorisation from the Office prior to processing personal data in order to ensure compliance of the intended processing with this Act and in particular to mitigate the risks involved for the data subjects where a controller or processor cannot provide for the appropriate safeguards referred to in section 36 in relation to the transfer of personal data to another country.

(2) The controller or processor shall consult the Office prior to processing personal data in order to ensure compliance of the intended processing with this Act and in particular to mitigate the risks involved for the data subjects where –

(a) a data protection impact assessment as provided for in section 34 indicates that processing operations are by virtue of their nature, scope or purposes, likely to present a high risk; or

(b) the Office considers it necessary to carry out a prior consultation on processing operations that are likely to present a high risk to the rights and freedoms of data subjects by virtue of their nature, scope or purposes.

(3) Where the Office is of the opinion that the intended processing does not comply with this Act, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such non-compliance.

(4) The Office shall make public a list of the processing operations which are subject to prior consultation in accordance with subsection (2)(b).

(5) The controller or processor shall provide the Office with the data protection impact assessment provided for in section 34 and, on request, with any other information, so as to allow the Office to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.

PART VI – TRANSFER OF PERSONAL DATA OUTSIDE MAURITIUS

36. Transfer of personal data outside Mauritius

(1) A controller or processor may transfer personal data to another country where –

(a) he or it has provided to the Commissioner proof of appropriate safeguards with respect to the protection of the personal data;

(b) the data subject has given explicit consent to the proposed transfer, after having been informed of the possible risks of the transfer owing to the absence of appropriate safeguards;

(c) the transfer is necessary –

(i) for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

(ii) for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person;

(iii) for reasons of public interest as provided by law;

(iv) for the establishment, exercise or defence of a legal claim; or

(v) in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or

(vi) for the purpose of compelling legitimate interests pursued by the controller or the processor which are not overridden by the interests, rights and freedoms of the data subjects involved and where –

(A) the transfer is not repetitive and concerns a limited number of data subjects; and

(B) the controller or processor has assessed all the circumstances surrounding the data transfer operation and has, based on such assessment, provided to the Commissioner proof of appropriate safeguards with respect to the protection of the personal data; or

(d) the transfer is made from a register which, according to law, is intended to provide information to the public and which is open for consultation by the public or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down by law for consultation are fulfilled in the particular case.

(2) A transfer pursuant to subsection (1)(d) shall not involve the entirety of the personal data or entire categories of the personal data contained in the register and, where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or in case they are to be the recipients.

(3) Subsection (1)(a) and (c)(i), (ii) and (vi) shall not apply to activities carried out by a public authority in the exercise of its functions.

(4) The Commissioner may request a person who transfers data to another country to demonstrate the effectiveness of the safeguards or the existence of compelling legitimate interests and may, in order to protect the rights and fundamental freedoms of data subjects, prohibit, suspend or subject the transfer to such conditions as he may determine.

PART VII – RIGHTS OF DATA SUBJECTS

37. Right of access

(1) (a) Every controller shall, on the written request of a data subject provide, at reasonable intervals, without excessive delay and, subject to subsection (7), free of charge, confirmation as to whether or not personal data relating to the data subject are being processed and forward to him a copy of the data.

(b) Where a controller has a reasonable doubt concerning the identity of a person making a request under paragraph (a), he or it may request the provision of additional information to confirm the identity of the data subject.

(2) Where personal data are being processed, the controller shall provide to the data subject information relating to –

(a) the purpose of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the data have been or will be disclosed;

(d) the period for which the data will be stored or, if this is not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to the processing of the data;

(f) the right to lodge a complaint with the Commissioner;

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision making, including profiling, and information about the logic involved, as well as the significance and envisaged consequences of such processing for the data subject; and

(i) appropriate safeguards taken under section 36, in case the personal data are transferred or intended to be transferred to another country.

(3) The controller shall provide the information referred to in subsection (2) in an intelligible form, using clear and plain language.

(4) Where the personal data are not or have not been collected from the data subject, the controller shall not be required to provide information where the processing is expressly prescribed by law or this proves to be impossible or involves a disproportionate effort.

(5) (a) The controller shall, within one month of the receipt of a request, inform the data subject in writing, whether or not any action has been taken pursuant to subsection (1).

(b) The period specified in paragraph (a) may be extended by a further month where necessary, taking into account the complexity and the number of requests made.

(6) Where a controller refuses to take action on the request of a data subject, he or it shall, within one month of the receipt of the request, inform the data subject in writing of the reason for the refusal and on the possibility of lodging a complaint with the Commissioner.

(7) (a) Where the request is manifestly excessive, the controller may charge a fee for providing the information or taking the action requested, or he or it may not take the action requested.

(b) Where the controller takes a decision under paragraph (a), he or it shall bear the burden of proving the manifestly excessive character of the request.

38. Automated individual decision making

(1) Every data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or significantly affects him.

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

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

(b) authorised by a law to which the controller is subject and which lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests; or

(c) based on the data subject's explicit consent.

(3) Any automated processing of personal data intended to evaluate certain personal aspects relating to an individual shall not be based on special categories of personal data.

(4) In the cases referred to in subsection (2), the information to be provided by the controller under section 23 shall include information as to the existence of processing for a decision of the kind referred to in subsection (1) and the envisaged effects of such processing on the data subject.

(5) In the cases referred to in subsection (2)(a) or (c), the controller shall implement suitable measures to safeguard the data subject's rights, freedoms and legitimate interests.

39. Rectification, erasure or restriction of processing

(1) (a) A controller shall, on being informed of the inaccuracy of personal data by a data subject to whom such data pertains, cause the data to be rectified without undue delay.

(b) A right to rectification under paragraph (a) shall include the right of a data subject to have incomplete personal data completed, having regard to the purpose of the processing.

(2) A controller shall erase personal data without undue delay where –

(a) the data are no longer necessary in relation to the purpose for which they were collected or otherwise processed;

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

(c) the data subject objects to the processing of personal data and there are no overriding legitimate grounds for the processing; or

(d) the personal data have been unlawfully processed.

(3) Where the controller has made the personal data public, he shall take all reasonable steps to inform third parties processing such data, that the data subject has requested the erasure of any links to, or copy or replication of, that personal data.

(4) Subsections (2) and (3) shall not apply where the processing of the personal data is necessary –

(a) for reasons of public interest in the field of public health;

(b) for the purpose of historical, statistical or scientific research;

(c) for compliance with a legal obligation to process the personal data to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or

(d) for the establishment, exercise or defence of a legal claim.

(5) A controller may, at the request of a data subject, restrict the processing of personal data where –

(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;

(b) the controller no longer needs the personal data for the purpose of the processing, but the data subject requires them for the establishment, exercise or defence of a legal claim;

(c) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; or

(d) the data subject has objected to the processing pursuant to section 41 pending verification as to whether the legitimate grounds of the controller override those of the data subject.

(6) Where processing of personal data is restricted under subsection (4) –

(a) the personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of a legal claim, the protection of the rights of another person or for reasons of public interest; and

(b) the controller shall inform the data subject before lifting the restriction on processing of the personal data.

(7) The controller shall implement mechanisms to ensure that the time limits established for the rectification, erasure or restriction of processing of personal data, or for a periodic review of the need for the storage of the personal data, are observed.

40. Right to object

(1) The data subject shall have the right to object in writing at any time to the processing of personal data concerning him unless the controller demonstrates compelling legitimate grounds for the processing which override the data subject's interests, rights and freedoms or for the establishment, exercise or defence of a legal claim.

(2) Where personal data are processed for the purpose of direct marketing, the data subject may object to processing of personal data concerning him for such marketing, which includes profiling to the extent that it is related to such direct marketing.

(3) Where a data subject objects to processing of personal data for the purpose of direct marketing, the personal data shall no longer be processed for that purpose.

(4) The rights referred to in subsections (1) and (2) shall be explicitly brought to the attention of the data subject.

(5) In this section –

"direct marketing" means the communication of any advertising or marketing material which is directed to any particular individual.

41. Exercise of rights

Any right conferred on an individual in this Act may be exercised –

(a) where the data subject is a minor, by a person who has parental authority over the minor or has been appointed as his guardian;

(b) where the data subject is physically or mentally unfit, by a person who has been appointed as his guardian or legal administrator by a Court; or

(c) in any other case, by a person duly authorised in writing by the data subject to make a request under this Part.

PART VIII – OTHER OFFENCES AND PENALTIES

42. Unlawful disclosure of personal data

(1) Any controller who, without lawful excuse, discloses personal data in any manner that is incompatible with the purpose for which such data has been collected shall commit an offence.

(2) Any processor who, without lawful excuse, discloses personal data processed by him without the prior authority of the controller on whose behalf the data are being or have been processed shall commit an offence.

(3) Subject to subsection (4), any person who –

(a) obtains access to personal data, or obtains any information constituting such data, without the prior authority of the controller or processor by whom the data are kept; and

(b) discloses the data or information to another person,

shall commit an offence.

(4) Subsection (3) shall not apply to a person who is an employee or agent of a controller or processor and is acting within his mandate.

(5) Any person who offers to sell personal data where such personal data has been obtained in breach of subsection (1) shall commit an offence.

(6) For the purpose of subsection (5), an advertisement indicating that personal data is or may be for sale constitutes an offer to sell the personal data.

43. Offence for which no specific penalty provided

(1) Any person who commits an offence under this Act for which no specific penalty is provided or who otherwise contravenes this Act shall, on conviction, be liable to a fine not exceeding 200, 000 rupees and to imprisonment for a term not exceeding 5 years.

(2) In addition to any penalty referred to in subsection (1), the Court may –

(a) order the forfeiture of any equipment or any article used or connected in any way with the commission of an offence;

(b) order or prohibit the doing of any act to stop a continuing contravention.

PART IX – MISCELLANEOUS

44. Exceptions and restrictions

(1) No exception to this Act shall be allowed except where it constitutes a necessary and proportionate measure in a democratic society for –

(a) subject to subsection (4), the protection of national security, defence or public security;

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

(c) an objective of general public interest, including an economic or financial interest of the State;

(d) the protection of judicial independence and judicial proceedings; or

(e) the protection of a data subject or the rights and freedoms of others.

(2) The processing of personal data for the purpose of historical, statistical or scientific research may be exempt from the provisions of this Act where the security and organisational measures specified in section 31 are implemented to protect the rights and freedoms of data subjects involved.

(3) Where this section has been breached, a data subject or the Commissioner may apply for a Judge's order to protect the rights of individuals.

(4) (a) Personal data shall be exempt from any provision of this Act where the non-application of such provision would, in the opinion of the Prime Minister, be required for the purpose of safeguarding national security, defence or public security.

(b) In any proceedings in which the non-application of any provision of this Act on grounds of national security, defence or public security is in question, a certificate under the hand of the Prime Minister certifying that the non-application of the provision is required for the purpose of safeguarding national security, defence or public security shall be conclusive evidence of that fact.

45. Annual report

(1) The Commissioner shall, not later than 3 months after the end of every year, lay an annual report of the activities of the Office before the National Assembly.

(2) The report shall include –

(a) a statement about the operation of Codes of Practice issued or approved, or Guidelines issued, by the Commissioner;

(b) any recommendations that the Commissioner thinks fit, in relation to compliance with this Act.

46. Compliance audit

The Commissioner may carry out periodical audits of the systems of controllers or processors to ensure compliance with this Act.

47. Codes and Guidelines

(1) The Commissioner may, for the purposes of this Act, issue or approve Codes of Practice, or issue Guidelines.

(2) The Commissioner may, before issuing or approving a Code of Practice, or issuing Guidelines, consult such person or authority as he thinks fit.

(3) Any Code of Practice –

(a) may be varied or revoked;

(b) shall, where it is approved under subsection (1),

come into operation on a day specified by the Commissioner.

48. Certification

(1) The Office may, in order to encourage compliance of processing operations by controllers and processors with this Act, lay down technical standards for data protection certification mechanisms and data protection seals and marks.

(2) A certification shall be –

(a) voluntary;

(b) issued to a controller or processor for a maximum period of 3 years and may be renewed under the same conditions where the relevant requirements continue to be met;

(c) withdrawn where the requirements for the certification are no longer met.

(3) Where a controller or processor seeks certification under this section, he or it shall provide to the Office all information and access to his or its processing activities which are necessary to conduct the certification procedure.

(4) A certification issued under this section shall not alter the responsibility of the controller or processor for compliance with this Act.

49. Confidentiality and oath

(1) The Commissioner and every authorised officer shall take the oath as set out in the Schedule.

(2) No person who is or has been the Commissioner or an authorised officer shall, except –

(a) in accordance with this Act or any other enactment;

(b) on the order of a Court or Judge,

divulge any confidential information obtained in the exercise of a power or in the performance of a duty under this Act.

(3) Any person who, without lawful excuse, contravenes subsection (2) shall commit an offence and shall, on conviction, be liable to a fine not exceeding 50, 000 rupees and to imprisonment for a term not exceeding 2 years.

50. Protection from liability

(1) Notwithstanding the Public Officers' Protection Act, where any action has been entered before a Court pursuant to an act done by the Commissioner or an authorised officer in the execution of his duties under this Act and it appears to the Court that there was reasonable cause to do such act, the Court shall so declare and thereafter the Commissioner or authorised officer shall be immune from all proceedings, whether civil or criminal, on account of such act.

(2) No liability, civil or criminal, shall attach to the Commissioner in respect of any act which he may have done or omitted to do in good faith in the execution, or purported execution, of his duties or powers under this Act.

51. Right of appeal

Any person aggrieved by a decision of the Commissioner under this Act may, within 21 days from the date when the decision is made known to that person, appeal to the Tribunal.

52. Special jurisdiction of Tribunal

(1) Subject to subsections (2) and (3), the Tribunal shall hear and dispose of any appeal under this Act.

(2) Sections 40 to 44 of the Information and Communication Technologies Act shall, as far as appropriate, apply to an appeal made under this Act and to such decision as may be reached by the Tribunal on appeal under this Act.

(3) Sections 39 and 42 (5) of the Information and Communication Technologies Act shall not apply to an appeal under this Act.

(4) Subject to subsection (5), every appeal under this Act shall be in such form and be accompanied by such fees as may be prescribed.

(5) The Tribunal may entertain an appeal after the expiry of the period of 21 days where it is satisfied that there was sufficient cause for not lodging the appeal within that period.

(6) The Tribunal may, after giving the parties to the appeal an opportunity of being heard, pass such orders as it thinks fit, confirming, varying or setting aside the decision appealed against.

(7) The Tribunal shall send a copy of every order made by it to the parties to the appeal.

(8) Any appeal lodged with the Tribunal under this Act shall be dealt with by it as expeditiously as possible and the Tribunal shall endeavour to dispose of the appeal within 6 weeks from the date the appeal was lodged.

(9) Any person who does not comply with an order issued by the Tribunal under subsection (6) shall commit an offence.

(10) No appeal shall lie against any decision made by the Tribunal following a settlement reached with the consent of the parties or their representatives.

53. Prosecution and jurisdiction

(1) An authorised officer may swear an information in respect of an offence under this Act or any regulations made under it before a Magistrate.

(2) Notwithstanding any other enactment, the Intermediate Court shall have jurisdiction to try an offence under this Act or any regulations made under it.

(3) No prosecution shall be instituted under this Act except by, or with the consent of, the Director of Public Prosecutions.

54. Certificate issued by Commissioner

In any proceedings –

(a) a copy of, or of an extract from, an entry in the register duly certified by the Commissioner to be a true copy shall be evidence of the entry or extract; and

(b) a certificate signed by the Commissioner and stating that there is not an entry in the register in respect of a specified person as a controller or processor shall be evidence of that fact.

55. Regulations

(1) The Minister may, for the purposes of this Act, after consultation with the Commissioner, make such regulations as he thinks fit.

(2) Any regulations made under subsection (1) may provide –

(a) for the amendment of the Schedule;

(b) for the requirements which are imposed on a controller or processor when processing personal data;

(c) for the contents which a notice or registration by a controller or processor should contain;

(d) for the information to be provided to a data subject and how such information shall be provided;

(e) for the levying of fees and taking of charges;

(f) for the issuing and approval of Codes of Practice and Guidelines; or

(g) that any person who contravenes them shall commit an offence and shall, on conviction, be liable to a fine not exceeding 100, 000 rupees and to imprisonment for a term not exceeding 5 years.

56. Repeal

The Data Protection Act is repealed.

57. Transitional provisions

(1) In this section –

"repealed Act" means the Data Protection Act.

(2) All assets and funds of the Data Protection Office under the repealed Act shall, at the commencement of this Act, remain vested in the Office.

(3) All rights, obligations and liabilities subsisting in favour of or against the Data Protection Office under the repealed Act shall, at the commencement of this Act, continue to exist under the same terms and conditions in favour of or against the Office.

(4) The contents of the register of controllers and processors kept under the repealed Act shall, at the commencement of this Act, be transferred to the register kept under this Act.

(5) Any registration granted under the repealed Act, which is valid at the commencement of this Act, shall be deemed to have been granted under this Act.

(6) Any application made to the Data Protection Office under the repealed Act and which is pending at the commencement of this Act shall be dealt with in accordance with this Act.

(7) Any Code of Practice or Guideline issued under the repealed Act shall, at the commencement of this Act, continue to remain in force.

(8) Any act or thing done, or any contract or agreement entered into, by the Data Protection Office shall, at the commencement of this Act, be deemed to have been done or entered into by the Office.

(9) All proceedings, judicial or otherwise, initiated before and pending at the commencement of this Act, by or against the Data Protection Office or the Commissioner, may be continued, by or against the Office or the Commissioner, as the case may be.

(10) For the purpose of section 45, the period starting from the commencement of this Act to the end of the year of such commencement shall be deemed to be the first year for the filing of the annual report.

(11) Where this Act does not make provision for any transition, the Minister may make such regulations as may be necessary for such transition.

58. Commencement

(1) Subject to subsection (2), this Act shall come into operation on a date to be fixed by Proclamation.

(2) Different dates may be fixed for the coming into operation of different sections of this Act.

Passed by the National Assembly on the eighth day of December two thousand and seventeen.

Bibi Safeena Lotun (Mrs)
Clerk of the National Assembly

SCHEDULE
[Section 49]

I, ...……, make oath/solemnly affirm/declare that I will faithfully and honestly fulfil my duties as authorised officer/Commissioner in conformity with the Data Protection Act 2017 and that I shall not, without the due authority in that behalf, disclose or make known any matter or thing which comes to my knowledge by reason of my duties as such.

…….
District Magistrate Port Louis