

DATA PROTECTION ACT

Act 13 of 2004 – 27 December 2004

(unless otherwise indicated)

ARRANGEMENT OF SECTIONS

SECTION

	PART I – PRELIMINARY	29.	Unlawful disclosure of personal data
1.	Short title		
2.	Interpretation	30.	Processing of personal data for direct marketing
3.	Application of Act	31.	Transfer of personal data
	PART II – DATA PROTECTION OFFICE	32.	Data matching
4.	Data Protection Office		PART V – THE DATA PROTECTION REGISTER
5.	Functions of Commissioner	33.	Register of data controllers and data processors
6.	Confidentiality and oath	34.	Application for registration
	PART III – POWERS OF COMMISSIONER	35.	Particulars to be furnished by data controller
7.	Powers of Commissioner	35A.	Particulars to be furnished by data processor
8.	Powers to obtain information	35B.	Registration of changes in particulars
9.	Delegation of powers by Commissioner	36.	Contents of register
10.	Contents of notice	37.	Inspection of register
11.	Complaints	38.	Duration of registration
12.	Enforcement of notice	39.	Failure to register or to renew registration
13.	Preservation Order	40.	Certificate issued by Commissioner
14.	Power to carry out prior security checks		PART VI – RIGHTS OF DATA SUBJECTS
15.	Compliance audit	41.	Access to personal data
16.	Powers to request assistance	42.	Compliance with request for access to personal data
17.	Powers of entry and search	43.	Denial of access to personal data
18.	–	44.	Inaccurate personal data
19.	Obstruction of authorised officer		PART VII – EXEMPTIONS
20.	Referral to police	45.	National security
21.	–	46.	Crime and taxation
	PART IV – OBLIGATION ON DATA CONTROLLERS	47.	Health and social work
22.	Collection of personal data	48.	Regulatory activities
23.	Accuracy of personal data	49.	Journalism, literature and art
24.	Processing of personal data	50.	Research, history and statistics
25.	Processing of sensitive personal data	51.	Information available to public under an enactment
26.	Use of personal data		
27.	Security of personal data		
28.	Duty to destroy personal data		

SECTION

52. Disclosure required by law or in connection with legal proceedings	60. Immunity and protection from liability
53. Legal professional privilege	61. Offences and penalties
54. Domestic purposes	62. Forfeiture
PART VIII – MISCELLANEOUS	63. Prosecution and jurisdiction
55. Annual report	64. Consequential amendments
56. Codes and guidelines	65. Regulations
57. Service of notice	66. Commencement
58. Right of Appeal	FIRST SCHEDULE
59. Special jurisdiction of Tribunal	SECOND SCHEDULE

DATA PROTECTION ACT

PART I – PRELIMINARY

1. Short title

This Act may be cited as the Data Protection Act.

(S. 1 came into operation on 27 December 2004.)

2. Interpretation

In this Act—

“adverse action”, in relation to a data subject, means any action that may adversely affect the person’s rights, benefits, privileges, obligations or interests;

“authorised officer” means an officer to whom the Commissioner has delegated his powers under section 9;

“blocking”, in relation to personal data, means suspending the modification of data, or suspending or restricting the provision of information to a third party where such provision is suspended or restricted in accordance with this Act;

“collect” does not include receipt of unsolicited information;

“Commissioner” means the Data Protection Commissioner referred to in section 4;

“computer” means any device for storing and processing information, whether or not the information is derived from other information by calculation, comparison or otherwise;

“consent” means any freely given specific and informed indication of the wishes of the data subject by which he signifies his agreement to personal data relating to him being processed;

“data” means information in a form which—

- (a) (i) is capable of being processed by means of equipment operating automatically in response to instructions given for that purpose; and
- (ii) is recorded with the intent of it being processed by such equipment; or
- (b) is recorded as part of a relevant filing system or intended to be part of a relevant filing system;

“data controller” means a person who, either alone or jointly with any other person, makes a decision with regard to the purposes for which and in the manner in which any personal data are, or are to be, processed;

“data matching procedure” means any procedure, whether manually or by means of any electronic or other device, whereby personal data collected for one or more purposes in respect of 10 or more data subjects are compared with personal data collected for any other purpose in respect of those data subjects where the comparison—

- (a) is for the purpose of producing or verifying data that; or
- (b) produces or verifies data in respect of which it is reasonable to believe that it is practicable that the data,

may be used, whether immediately or at any subsequent time, for the purpose of taking any adverse action against any of those data subjects;

“data processor” means a person, other than an employee of the data controller, who processes the data on behalf of the data controller;

“Data Protection Principles” means the Data Protection Principles specified in the First Schedule;

“data subject” means a living individual who is the subject of personal data;

“direct marketing” means the communication of any advertising or marketing material which is directed to any particular individual;

“document” includes—

- (a) a disc, tape or any other device in which the data 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 as to be capable, with or without the aid of some other equipment, of being reproduced from the film, tape or other device;

“inaccurate”, in relation to personal data, means incorrect, misleading, incomplete or obsolete;

“individual” means a living individual;

“information and communication network” means a network for the transmission of messages and includes a telecommunication network;

“information and communication technologies” —

- (a) means technologies employed in collecting, storing, using or sending out information; and
- (b) includes those involving the use of computers or any telecommunication system;

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

“Office” means the Data Protection Office established under section 4;

“personal data” means—

- (a) data which relate to an individual who can be identified from those data; or
- (b) data or other information, including an opinion forming part of a database, whether or not recorded in a material form, about an individual whose identity is apparent or can reasonably be ascertained from the data, information or opinion;

“proceedings” —

- (a) means any proceedings conducted by or under the supervision of a Judge, Magistrate or judicial officer; and
- (b) includes—
 - (i) any inquiry or investigation into a criminal offence; and
 - (ii) any disciplinary proceedings;

“processing” means any operation or set of operations which is performed on the data wholly or partly by automatic means, or otherwise than by automatic means, and includes—

- (a) collecting, organising or altering the data;
- (b) retrieving, consulting, using, storing or adapting the data;
- (c) disclosing the data by transmitting, disseminating or otherwise making it available; or
- (d) aligning, combining, blocking, erasing or destroying the data;

“register” means the register referred to in section 33;

“relevant filing system” means a structured set of information relating to individuals that, although it is not in a form capable of being processed automatically, is structured, either by reference to any individual or by reference to criteria relating to the individual, in such a way that the structure allows ready accessibility to information relating to that individual;

“relevant function” means—

- (a) any function conferred on any person by or under any enactment;
- (b) any function of any Minister; or
- (c) any other function which is of a public nature and is exercised in the public interest;

“relevant person”, in relation to a data subject, means—

- (a) where the data subject is a minor, a person who has parental authority over the minor or has been appointed as his guardian by the Court;
- (b) where the data subject is physically and mentally unfit, a person who has been appointed as his guardian by the Court;
- (c) in any other case, a person duly authorised in writing by the data subject to make a request under sections 41 and 44;

“sensitive personal data” means personal information concerning a data subject and consisting of information as to—

- (a) his racial or ethnic origin;
- (b) his political opinion or adherence;
- (c) his religious belief or other belief of a similar nature;
- (d) his membership of a trade union;
- (e) his physical or mental health;
- (f) his sexual preferences or practices;
- (g) the commission or alleged commission of an offence by him; or
- (h) 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 such proceedings;

“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 electromagnetic energy or both;

“third party”, in relation to personal data, means any person other than—

- (a) the data subject;
- (b) a relevant person in the case of a data subject;
- (c) the data controller; or
- (d) a person authorised in writing by the data controller to collect, hold, process or use the data—
 - (i) under the direct control of the data controller; or
 - (ii) on behalf of the data controller;

“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 36 of the Information and Communication Technologies Act;

“underlying service” means the type of service that is used within the computer system;

“use”, in relation to personal data, includes disclose or transfer the data.

[S. 2 amended by s. 2 (a) of Act 1 of 2009 w.e.f. 22 May 2009.]

(S. 2 came into operation on 27 December 2004.)

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) Subject to Part VII, this Act shall apply to a data controller—

- (a) who is established in Mauritius and processes data in the context of that establishment; and
- (b) who is not established in Mauritius but uses equipment in Mauritius for processing data, other than for the purpose of transit through Mauritius.

(4) A data controller referred to in subsection (3) (b) shall nominate, for the purposes of this Act, a representative established in Mauritius.

(5) For the purposes of subsection (3) (a), any person who—

- (a) is ordinarily resident in Mauritius;
- (b) carries out data processing activities through an office, branch or agency in Mauritius,

shall be treated as being established in Mauritius.

(6) Subject to the provisions of this Act, every data controller and data processor shall comply with the Data Protection Principles.

[S. 3 amended by s. 2 (b) of Act 1 of 2009 w.e.f. 22 May 2009.]

(S. 3 came into operation on 16 February 2009.)

PART II – DATA PROTECTION OFFICE

4. Data Protection Office

(1) There is established for the purposes of this Act a Data Protection Office which shall be a public office.

(2) The head of the Office shall be known as the Data Protection Commissioner.

(3) The Commissioner shall be a barrister with at least 5 years' standing at the Bar.

(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.

(S. 4 came into operation on 27 December 2004.)

5. Functions of Commissioner

The Commissioner shall—

- (a) ensure compliance with this Act and any regulations made under the Act;
(Para. (a) came into operation on 16 February 2009.)
- (b) issue or approve codes of practice or guidelines for the purposes of this Act;
(Para. (b) came into operation on 27 December 2004.)
- (c) create and maintain a register of all data controllers and data processors;
(Para. (c) came into operation on 27 December 2004.)
- (d) exercise control on all data processing activities, either of its own motion or at the request of a data subject, and verify whether the processing of data is in accordance with this Act or regulations made under the Act;
(Para. (d) came into operation on 16 February 2009.)
- (e) promote self-regulation among data controllers and data processors;
(Para. (e) came into operation on 27 December 2004.)
- (f) investigate any complaint or information which give rise to a suspicion that an offence gives under this Act may have been, is being or is about to be committed;
(Para. (f) came into operation on 16 February 2009.)
- (g) take such measures as may be necessary to bring to the knowledge of the general public the provisions of this Act;
(Para. (g) came into operation on 27 December 2004.)
- (h) undertake research into, and monitor developments in, data processing, including data-matching, data linkage and information and communication technologies, and ensure that there are no significant risks or any adverse effects of those developments on the privacy of individuals;
(Para. (h) came into operation on 27 December 2004.)
- (i) examine any proposal for data matching or data linkage that may involve an interference with or may otherwise have adverse effects on the privacy of individuals and ensure that any adverse

effects of such proposal on the privacy of individuals are minimised;

(Para. (i) came into operation on 27 December 2004.)

- (ia) co-operate 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;
- (j) 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.

(Para. (j) came into operation on 27 December 2004.)

[S. 5 amended by s. 2 (c) of Act 1 of 2009 w.e.f. 22 May 2009; s. 10 (a) of Act 14 of 2009 w.e.f. 30 July 2009.]

6. Confidentiality and oath

(1) The Commissioner and every officer of the Office shall take the oath specified in the Second Schedule.

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

- (a) in accordance with this Act or any other enactment;
- (b) upon a Court order; or
- (c) as authorised by the order of a Judge,

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

(3) Where the Commissioner or any authorised officer, otherwise than in the course of his duties, uses or records personal data or sensitive personal data, that comes to his knowledge or to which he has access by reason of his position as Commissioner or authorised officer, he shall commit an offence.

(4) 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.

[S. 6 amended by s. 2 (d) of Act 1 of 2009 w.e.f. 22 May 2009.]

(S. 6 came into operation on 27 December 2004.)

PART III – POWERS OF COMMISSIONER

7. Powers of Commissioner

The Commissioner shall have power, for the purpose of carrying out his functions, to do all such acts as appear to him to be requisite, advantageous or convenient for, or in connection with, the carrying out of these functions.

(S. 7 came into operation on 16 February 2009.)

8. Powers to obtain information

Subject to section 26 of the Bank of Mauritius Act, section 64 of the Banking Act, section 83 of the Financial Services Act and section 30 of the Financial Intelligence and Anti-Money Laundering Act—

- (a) the Commissioner may, by notice in writing served on any person, request from that person, such information as is necessary or expedient for the performance of his functions and exercise of his powers under this Act; and
- (b) where the information requested by the Commissioner is stored in a computer, disc, 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.

[S. 8 repealed and replaced by s. 10 (b) of Act 14 of 2009 w.e.f. 30 July 2009.]

(S. 8 came into operation on 16 February 2009.)

9. Delegation of powers by Commissioner

The Commissioner may delegate any of the investigating and enforcement powers conferred upon him by this Act to any officer of his Office and to any police officer designated for that purpose by the Commissioner of Police.

(S. 9 came into operation on 16 February 2009.)

10. Contents of notice

(1) Subject to subsection (2)—

- (a) the notice specified in section 8 shall state that the person to whom the notice is addressed has a right of appeal conferred under section 58; and
- (b) the delay granted for compliance shall not be less than 21 days.

(2) Where a notice of appeal against a decision made under section 8 is lodged with the Commissioner, the information required need not be furnished, pending the determination or withdrawal of the appeal.

(3) Where the Commissioner considers that the information is required urgently for the proper performance of his functions and exercise of his powers under this Act, the Commissioner may apply to the Judge in Chambers for communication of the information.

(4) 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.

(S. 10 came into operation on 16 February 2009.)

11. Complaints

Where a complaint is made to the Commissioner that this Act or any regulation made under it has been, is being or is about to be contravened, the Commissioner shall—

- (a) investigate the complaint or cause it to be investigated by an authorised officer, unless he is of the opinion that such complaint is frivolous or vexatious; and
- (b) as soon as reasonably practicable, notify the complainant in writing of his decision in relation to the complaint and that the complainant may, if he is aggrieved by the Commissioner's decision, appeal to the Tribunal.

(S. 11 came into operation on 16 February 2009.)

12. Enforcement of notice

(1) Where the Commissioner is of opinion that a data controller or a data processor has contravened, is contravening or is about to contravene this Act, the Commissioner may serve an enforcement notice on the data controller or the data processor, as the case may be, requiring him to take such steps within such time 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 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 matter, as the case may be, which makes it likely that a contravention will arise;
- (c) specify a time limit which shall not be less than 21 days within which those measures shall be implemented; and
- (d) state the right of appeal conferred under section 58.

(4) In complying with an enforcement notice served under subsection (1), a data controller or a data processor, as the case may be, shall, as soon as practicable and in any event not later than 21 days after such 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 enforcement notice and ending immediately before such compliance,

of any amendment.

(5) Where the Commissioner considers that any provision of the enforcement notice need not be complied with to ensure compliance with the Data Protection Principles to which the notice relates, he may vary the notice and, where he does so, he shall notify in writing 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.

(S. 12 came into operation on 16 February 2009.)

13. Preservation Order

(1) The Commissioner may apply to a Judge in Chambers for an order for the expeditious preservation of data, including traffic data, where he has reasonable grounds to believe that such data is vulnerable to loss or modification.

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

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

(S. 13 came into operation on 16 February 2009.)

14. Power to carry out prior security checks

(1) Where the Commissioner is of the opinion that the processing or transfer of data by a data controller or data processor entails specific risks to the privacy rights of data subjects, he may inspect and assess the security measures taken under section 27 prior to the beginning of the processing or transfer.

continued on page D3 – 11

(2) The Commissioner may, at any reasonable time during working hours, carry out further inspection and assessment of the security measures imposed on a data controller or data processor under section 27.

[S. 14 amended by s. 10 (c) of Act 14 of 2009 w.e.f. 30 July 2009.]

(S. 14 came into operation on 16 February 2009.)

15. Compliance audit

The Commissioner may carry out periodical audits of the systems of data controllers or data processors to ensure compliance with Data Protection Principles.

[S. 15 amended by s. 10 (d) of Act 14 of 2009 w.e.f. 30 July 2009.]

(S. 15 came into operation on 16 February 2009.)

16. Powers to request assistance

(1) For the purposes of gathering information or for the proper conduct of any investigation concerning compliance with this Act, the Commissioner may seek the assistance of such persons or authorities as he thinks fit and that person or authority may do such things as are reasonably necessary to assist the Commissioner in the performance of the Commissioner's functions.

(2) Any person assisting the Commissioner pursuant to subsection (1) shall, for the purposes of section 6, be deemed to an officer of the Office.

(S. 16 came into operation on 16 February 2009.)

17. Powers of entry and search

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

(2A) 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.

(2B) A warrant issued under subsection (2A) shall be valid for the period stated in the warrant and may be subject to any condition which the Magistrate may specify.

(3) Subject to section 26 of the Bank of Mauritius Act, section 64 of the Banking Act, section 83 of the Financial Services Act and section 30 of the Financial Intelligence and Anti-Money Laundering 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 either orally or in writing.

(4) Where the information requested by the authorised officer pursuant to subsection (3) is stored in a computer, disc, 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.

(5) For the purpose of carrying out his duties under this section, the authorised officer may be accompanied by such person as the Commissioner thinks fit.

[S. 17 amended by s. 2 (e) of Act 1 of 2009 w.e.f. 22 May 2009; s. 10 (e) of Act 14 of 2009 w.e.f. 30 July 2009.]

(S. 17 came into operation on 16 February 2009.)

18. —

[S. 18 repealed by s. 2 (f) of Act 1 of 2009 w.e.f. 22 May 2009.]

(S. 18 came into operation on 16 February 2009.)

19. Obstruction of authorised officer

Any person who, in relation to the exercise of powers conferred by section 17—

- (a) obstructs or impedes an authorised officer in the exercise of any of his powers;
- (b) fails to provide assistance or information requested by the authorised officer;
- (c) refuses to allow an authorised officer to enter any premises or to take any person with him in the exercise of his functions;
- (d) gives to an authorised officer any information which is false and 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.

[S. 19 amended by s. 2 (g) of Act 1 of 2009 w.e.f. 22 May 2009.]

(S. 19 came into operation on 16 February 2009.)

20. Referral to police

On completion of an investigation under this Act, the Commissioner shall, where the investigation reveals that an offence may have been committed under this Act or any regulations made under the Act, refer the matter to the Police.

(S. 20 came into operation on 16 February 2009.)

21. —

[S. 21 repealed by s. 2 (h) of Act 1 of 2009 w.e.f. 22 May 2009.]

(S. 21 came into operation on 16 February 2009.)

PART IV – OBLIGATION ON DATA CONTROLLERS

22. Collection of personal data

(1) Subject to Part VII, a data controller shall not collect personal data unless—

- (a) it is collected for a lawful purpose connected with a function or activity of the data controller; and
- (b) the collection of the data is necessary for that purpose.

(2) Where a data controller collects personal data directly from a data subject, the data controller shall, at the time of collecting personal data, ensure that the data subject is informed of—

- (a) the fact that the data is being collected;
- (b) the purpose for which the data is being collected;
- (c) the intended recipients of the data;
- (d) the name and address of the data controller;
- (e) whether the supply of the data by the data subject is voluntary or mandatory;
- (f) the consequences for that data subject if all or any part of the requested data is not provided;
- (g) whether—
 - (i) the data collected shall be processed; and
 - (ii) the consent of the data subject shall be required for such processing; and
- (h) his right of access to, the possibility of correction of and destruction of, the personal data to be provided.

(3) A data controller shall not be required to comply with subsection (2)—

- (a) in respect of a data subject where—
 - (i) compliance with subsection (2) in respect of a second or subsequent collection will be to repeat, without any material difference, what was done to comply with that subsection in respect of the first collection; and
 - (ii) not more than 12 months have elapsed between the first collection and the second or subsequent collection;
- (b) where—
 - (i) compliance is not reasonably practicable at the time of collection, provided that the data controller makes available to the data subject all the relevant information specified in subsection (2) as soon as practicable; or
 - (ii) the data is used in a form in which the data subject cannot or could not reasonably expect to be identified.

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

(5) Subsection (3) shall not operate to prevent a second or subsequent collection from becoming a first collection where the data controller has complied with subsection (2) in respect of the second or subsequent collection.

(S. 22 came into operation on 16 February 2009.)

23. Accuracy of personal data

A data controller shall take every reasonable step to ensure that personal data within his possession—

- (a) is accurate; and
- (b) where such data requires regular updating, is kept up to date.

(S. 23 came into operation on 16 February 2009.)

24. Processing of personal data

(1) No personal data shall be processed unless the data controller has obtained the express consent of the data subject.

(2) Notwithstanding subsection (1), personal data may be processed without obtaining the express consent of the data subject where the processing is necessary—

- (a) for the performance of a contract to which the data subject is a party;
- (b) for the purpose of taking steps required by the data subject before entering into a contract;
- (c) for the purpose of protecting the vital interests of the data subject;
- (d) for compliance with any legal obligation to which the data controller is subject;
- (da) for the purpose of making use of a unique identification number to facilitate sharing information and avoid multiple registrations among public sector agencies;
- (e) for the administration of justice; or
- (f) in the public interest.

[S. 24 amended by s. 14 of Act 9 of 2015 w.e.f. 14 May 2015.]

(S. 24 came into operation on 16 February 2009.)

continued on page D3 – 15

25. Processing of sensitive personal data

(1) No sensitive personal data shall be processed unless the data subject—

- (a) gives his express consent to the processing of the personal data; or
- (b) makes the data public.

(2) Subsection (1) shall not apply where the processing—

- (a) is necessary—
 - (i) for exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with his employment;
 - (ii) in order to protect the vital interests of the data subject or another person in a case where consent cannot be given by or on behalf of the data subject, or the data controller cannot reasonably be expected to obtain the consent of the data subject;
 - (iii) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject is unreasonably withheld;
 - (iv) for the performance of a contract to which the data subject is a party;
 - (v) in order to take steps required by the data subject prior to entering into a contract;
 - (vi) for compliance with a legal obligation to which the data controller is subject;
- (b) is carried out by any charitable entity or any association which exists for political, philosophical, religious or trade union purposes, in the course of its legitimate activities and the processing—
 - (i) is carried out with the appropriate safeguards specified under sections 22, 23, 26 and 27;
 - (ii) is related only to individuals who are members of the charitable entity or association; and
 - (iii) does not involve disclosure of the personal data to a third party without the consent of the data subject;
- (c) is in respect of the information contained in the personal data made public as a result of steps deliberately taken by the data subject;
- (ca) is required by any investigatory authority under the Financial Intelligence and Anti-Money Laundering Act;
- (d) is required by law.

[S. 25 came into operation on 16 February 2009; amended by s. 10 of Act 27 of 2013 w.e.f. 21 December 2013.]

26. Use of personal data

The data controller shall ensure that personal data is—

- (a) kept only for one or more specified and lawful purposes for which the data is collected and processed;
- (b) not used or disclosed in any manner incompatible with the purposes for which the data is collected and processed;
- (c) adequate, relevant and not excessive in relation to the purposes for which the data is collected and processed; and
- (d) not kept for longer than is necessary for the purposes for which the data is collected and processed.

(S. 26 came into operation on 16 February 2009.)

27. Security of personal data

(1) A data controller shall—

- (a) take appropriate security and organisational measures for the prevention of unauthorised access to, alteration of, disclosure of, accidental loss, and 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 the unauthorised access to, alteration of, disclosure of, destruction of the data and its accidental loss; and
 - (ii) the nature of the data concerned.

(2) A data controller or a data processor shall take all reasonable steps to ensure that any person employed by him is aware of and complies with the relevant security measures.

(3) Where a data controller is using the services of a data processor, he shall choose a data processor providing sufficient guarantees in respect of security and organisational measures for the purposes of complying with subsection (1).

(4) Where the data controller is using the services of a data processor under subsection (3), the data controller and the data processor shall enter into a written contract which shall provide that—

- (a) the data processor shall act only on instructions received from the data controller; and
- (b) the data processor shall be bound by obligations devolving on the data controller under subsection (1).

(5) Without prejudice to subsection (1), in determining the appropriate security measures, in particular, where the processing involves the transmission of data over an information and communication network, a data 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.

(S. 27 came into operation on 16 February 2009.)

28. Duty to destroy personal data

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

- (a) destroy such data as soon as reasonably practicable; and
- (b) notify any data processor holding such data.

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

(S. 28 came into operation on 16 February 2009.)

29. Unlawful disclosure of personal data

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

(2) Any data processor who, without lawful excuse, discloses personal data processed by him without the prior authority of the data controller on whose behalf such data is or has 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 prior authority of the data controller or data processor by whom such data is 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 data 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 purposes of subsection (5), an advertisement indicating that personal data is or may be for sale constitutes an offer to sell the personal data.

(S. 29 came into operation on 16 February 2009.)

30. Processing of personal data for direct marketing

(1) A person may, at any time, by notice in writing, request a data controller—

- (a) to stop; or

- (b) not to begin,

the processing of personal data in respect of which he is a data subject, for the purposes of direct marketing.

(2) Where the data controller receives a request under subsection (1) (a), he shall, as soon as reasonably practicable and in any event not more than 28 days after the request has been received—

- (a) where the data are kept only for purposes of direct marketing, erase the data; and
- (b) where the data are kept for direct marketing and other purposes, stop processing the data for direct marketing.

(3) Where the data controller receives a request under subsection (1) (b), he—

- (a) shall, where the data are kept only for the purpose of direct marketing, as soon as reasonably practicable and in any event not more than 28 days after the request has been received, erase the data; or
- (b) shall not, where the data are kept for direct marketing and other purposes, process the data for direct marketing after the expiry of 28 days.

(4) The data controller shall notify the data subject in writing of any action taken under subsections (2) and (3) and, where appropriate, inform him of the other purposes for which the personal data is being processed.

(5) Where a data controller fails to comply with a notice under subsection (1), the data subject may appeal to the Tribunal.

(6) Where a data controller fails to comply with an order of the Tribunal, he shall commit an offence.

(S. 30 came into operation on 16 February 2009.)

31. Transfer of personal data

(1) Subject to subsection (2), no data controller shall, except with the written authorisation of the Commissioner, transfer personal data to another country.

(2) The Eighth Data Protection Principle shall not apply where—

- (a) the data subject has given his consent to the transfer;
- (b) the transfer is necessary—
 - (i) for the performance of a contract between the data subject and the data controller, or for the taking of steps at the request of the data subject with a view to his entering into a contract with the data controller;
 - (ii) for the conclusion of a contract between the data controller and a person, other than the data subject, which is entered at the request of the data subject, or is in the interest of the data subject, or for the performance of such a contract;

- (iii) in the public interest, to safeguard public security or national security;
- (c) the transfer is made on such terms as may be approved by the Commissioner to ensure the adequate safeguards for the protection of the rights of the data subject.

(3) For the purpose of subsection (2) (c), the adequacy of the level of protection of a country shall be assessed in the light of all the circumstances surrounding the data transfer, having regard in particular to—

- (a) the nature of the data;
- (b) the purpose and duration of the proposed processing;
- (c) the country of origin and country of final destination;
- (d) the rules of law, both general and sectoral, in force in the country in question; and
- (e) any relevant codes of conduct or other rules and security measures which are complied with in that country.

[S. 31 amended by s. 10 (f) of Act 14 of 2009 w.e.f. 30 July 2009.]

(S. 31 came into operation on 16 February 2009.)

32. Data matching

(1) No data controller shall carry out a data matching procedure unless—

- (a)
 - (i) the data subject whose personal data is the subject of that procedure has given his consent to the procedure being carried out;
 - (ii) the Commissioner has consented to the procedure being carried out; and
 - (iii) the procedure is carried out in accordance with such conditions as the Commissioner may impose; or
- (b) it is required or permitted under any other enactment.

(2) Subject to subsection (3), a data controller shall not take any adverse action against any data subject as a consequence of the carrying out of a data matching procedure—

- (a) unless the data controller has served a notice in writing on the data subject—
 - (i) specifying the adverse action it proposes to take and the reasons therefor;
 - (ii) stating that the data subject has 7 days after the receipt of the notice to show cause why the adverse action should not be taken; and
- (b) until the expiry of the 7 days specified in paragraph (a).

(3) Subsection (2) shall not preclude a data controller from taking any adverse action against any data subject if compliance with the requirements of that subsection shall prejudice any investigation into the commission of any offence which has been, is being or is likely to be committed.

(S. 32 came into operation on 16 February 2009.)

PART V – THE DATA PROTECTION REGISTER

33. Register of data controllers and data processors

(1) There shall be a register of data controllers and data processors to be known as the Data Protection Register, which shall be kept and maintained by the Commissioner.

(2) Subject to Part VII, every data controller and data processor shall, before keeping or processing personal data or sensitive personal data shall register himself with the Commissioner.

[S. 33 repealed and replaced by s. 2 (i) of Act 1 of 2009 w.e.f. 22 May 2009.]

(S. 33 came into operation on 16 February 2009.)

34. Application for registration

(1) Every data controller and data processor shall—

- (a) apply for registration in writing to the Commissioner; and
- (b) together with the application, provide the particulars specified, in the case of a data controller, in section 35 and, in the case of a data processor, in section 35A.

(2) Where any data controller or data processor intends to keep or process personal data or sensitive personal data for 2 or more purposes, he shall make an application for separate registration in respect of any of those purposes and entries shall be made in accordance with any such applications.

(3) Subject to subsection (4), the Commissioner shall grant an application for registration, unless he reasonably believes that—

- (a) the particulars proposed for inclusion in an entry in the register are insufficient or any other information required by the Commissioner either has not been furnished, or is insufficient;
- (b) appropriate safeguards for the protection of the privacy of the data subjects concerned are not being, or will not continue to be, provided by the data controller; or
- (c) the person applying for registration is not a fit and proper person.

(4) Upon registration of an application, the applicant shall pay such fee as may be prescribed.

(5) Where the Commissioner refuses an application for registration, he shall, as soon as reasonably practicable, notify in writing the applicant of the refusal—

- (a) specifying the reasons for the refusal; and

- (b) informing the applicant that he may appeal against the refusal under to section 58.

(6) The Commissioner may, at any time, at the request of the person to whom an entry in the register relates, remove his name from the register.

[S. 34 amended by s. 2 (j) of Act 1 of 2009 w.e.f. 22 May 2009.]

(S. 34 came into operation on 16 February 2009.)

35. Particulars to be furnished by data controller

(1) A data controller who applies for registration under section 34 shall provide the following particulars—

- (a) his name and address;
- (b) if he has nominated a representative for the purposes of this Act, the name and address of the representative;
- (c) a description of the personal data being or to be processed by or on behalf of the data controller, and of the category of data subjects, to which the personal data relate;
- (d) a statement as to whether or not he holds, or is likely to hold, sensitive personal data;
- (e) a description of the purpose for which the personal data are being or are to be processed;
- (f) a description of any recipient to whom the data controller intends or may wish to disclose the personal data;
- (g) the names, or a description of, any country to which the data controller directly or indirectly transfers, or intends or may wish, directly or indirectly, to transfer the data; and
- (h) the class of data subjects, or where practicable the names of data subjects, in respect of which the data controller holds personal data.

(2) Any data controller who knowingly supplies false information under 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 2 years.

(3) Where the data controller in respect of whom there is an entry in the register changes his address, he shall, within 15 days of the change in address, notify the Commissioner in writing.

[S. 35 amended by s. 2 (k) of Act 1 of 2009 w.e.f. 22 May 2009.]

(S. 35 came into operation on 16 February 2009.)

35A. Particulars to be furnished by data processor

(1) A data processor who applies for registration under section 34 shall provide the following particulars—

- (a) his name and address;

- (b) a description of the personal data being, or to be processed, and the category of data subjects to which the personal data relate;
- (c) the country to which he transfers, or intends to transfer, the personal data;
- (d) a statement as to whether or not he processes, or is likely to process, sensitive personal data; and
- (e) such other particulars as the Commissioner may require.

(2) Any data processor who knowingly supplies false information under 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 2 years.

(3) Where a data processor in respect of whom there is an entry in the register changes his address, he shall, within 15 days of the change in address, notify the Commissioner in writing.

[S. 35A inserted by s. 2 (l) of Act 1 of 2009 w.e.f. 22 May 2009.]

35B. Registration of changes in particulars

(1) Where, following the granting of an application under section 34, there is a change in any of the particulars referred to in section 35 or 35A, the data controller or data processor, as the case may be, shall, within 14 days of the date of the change, notify the Commissioner in writing of the nature and the date of the change.

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

(3) Any data controller or data 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.

[S. 35B inserted by s. 10 (g) of Act 14 of 2009 w.e.f. 30 July 2009.]

36. Contents of register

Each entry in the register shall contain the particulars provided under sections 35 and 35A.

[S. 36 amended by s. 2 (m) of Act 1 of 2009 w.e.f. 22 May 2009.]

(S. 36 came into operation on 16 February 2009.)

37. Inspection of register

(1) The register shall be kept in the office of the Commissioner and shall at all reasonable times be available for inspection by any person free of charge.

(2) 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.

(S. 37 came into operation on 16 February 2009.)

38. Duration of registration

(1) Any registration under section 34 shall be for a period not exceeding one year and on the expiry of such period, the relevant entry shall be cancelled unless the registration is renewed.

(2) The period specified under subsection (1) shall be calculated—

- (a) in the case of a first registration, from the date on which the relevant entry was made in the register; and
- (b) in the case of a registration which has been renewed, from the date on which it was renewed.

(3) The Commissioner may, subject to this Act, renew a registration upon application by any data controller or data processor and on payment of such fee as may be prescribed.

[S. 38 amended by s. 2 (n) of Act 1 of 2009 w.e.f. 22 May 2009.]

(S. 38 came into operation on 16 February 2009.)

39. Failure to register or to renew registration

Any data controller or data processor who, without reasonable excuse or lawful authority, keeps or processes any personal data or sensitive personal data, without registering himself or renewing his registration, shall commit an offence.

[S. 39 repealed and replaced by s. 2 (o) of Act 1 of 2009 w.e.f. 22 May 2009.]

(S. 39 came into operation on 16 February 2009.)

40. Certificate issued by Commissioner

In any proceedings in which the registration of a person as a data controller or a data processor is in question, a certificate under the hand of the Commissioner that there is no entry in the register in respect of the person as a data controller or data processor shall be conclusive evidence of that fact.

(S. 40 came into operation on 16 February 2009.)

PART VI – RIGHTS OF DATA SUBJECTS

41. Access to personal data

(1) Subject to section 42, a data controller shall, on the written request of a data subject or a relevant person—

- (a) inform the data subject or the relevant person—
 - (i) whether the data kept by him include personal data relating to the data subject;
 - (ii) of the purposes for which the data are being or are to be processed;

continued on page D3 – 23

(iii) of the recipients or classes of recipients to whom they are or may be disclosed; and

(b) supply the data subject or the relevant person with a copy of any data referred to in paragraph (a) on payment of the prescribed fee.

(2) A request under subsection (1) (a) and (b) shall be treated as a single request.

(3) Where any data referred to in subsection (1) is expressed in terms that are not intelligible without explanation, the data controller shall supply the information with an explanation of those terms.

(4) A fee paid by any person to a data controller under this section shall be returned to him where a request under subsection (1) is not complied with.

(5) The information to be supplied pursuant to a request under this section shall be supplied by reference to any personal data at the time when the request is received, except that it may take account of any amendment or deletion made between that time and the time when the information is supplied, being an amendment or deletion that would have been made regardless of the receipt of the request.

(S. 41 came into operation on 16 February 2009.)

42. Compliance with request for access to personal data

(1) Subject to subsection (2) and section 43 and to the payment of the prescribed fee, a data controller shall comply with a request under section 41 not later than 28 days after the receipt of the request.

(2) Where a data controller is unable to comply with the request within the period specified in subsection (1), he shall—

(a) before the expiry of the specified period—

(i) inform the data subject or the relevant person who has made the request on behalf of the data subject, that he is unable to comply with the request and shall, if required, state the reasons therefor;

(ii) endeavour to comply with the request in such time as may be reasonably practicable; and

(b) as soon as practicable after the expiry of the specified period, comply with the request.

(S. 42 came into operation on 16 February 2009.)

43. Denial of access to personal data

(1) A data controller may refuse a request under section 41 where—

(a) he is not supplied with such information as he may reasonably require in order to satisfy himself as to the identity of the person making the request, and to locate the information which the person seeks;

- (b) compliance with such request will be in contravention of his confidentiality obligation imposed under any other enactment.

(2) Where a data controller cannot comply with a request under section 41 without disclosing personal data relating to another person, he may refuse the request unless—

- (a) the other individual has consented to the disclosure of his personal data to the person making the request; or
- (b) he obtains the written approval of the Commissioner.

(3) In determining for the purposes of subsection (2) (b) whether it is reasonable for the Commissioner to approve a request without the consent of the other individual concerned, regard shall be had, in particular, to—

- (a) any duty of confidentiality owed to the other individual;
- (b) any steps taken by the data controller with a view to seeking the consent of the other individual;
- (c) whether the other individual is capable of giving consent; and
- (d) any express refusal of consent by the other individual.

(4) (a) Where a data controller has previously complied with a request made under section 41 by a data subject, the data controller is not obliged to comply with a subsequent identical or similar request under that section by that data subject unless a reasonable interval has elapsed between compliance with the previous request and the making of the current request.

(b) In determining, for the purposes of paragraph (a), whether requests under section 41 are made at reasonable intervals, regard shall be had to—

- (i) the nature of the data;
- (ii) the purpose for which the data are processed; and
- (iii) the frequency with which the data are altered.

(5) A data controller shall not comply with a request under section 41 where—

- (a) he is being requested to disclose information given or to be given in confidence for the purposes of—
 - (i) the education, training or employment, or prospective education, training or employment, of the data subject;
 - (ii) the appointment, or prospective appointment, of the data subject to any office; or
 - (iii) the provision, or prospective provision, by the data subject of any service;
- (b) the personal data requested consist of information recorded by candidates during an academic, professional or other examination;

- (c) such compliance would, by revealing evidence of the commission of any offence other than an offence under this Act, expose him to proceedings for that offence.

(S. 43 came into operation on 16 February 2009.)

44. Inaccurate personal data

(1) A data controller shall, upon being informed as to the inaccuracy of personal data, by a data subject to whom such data pertains, cause such data to be rectified, blocked, erased or destroyed, as appropriate.

(2) Where a data controller is aware that a third party holds inaccurate personal data, he shall, as soon as reasonably practicable, require the third party to rectify, block, erase or destroy the data, as appropriate.

(3) Where the third party specified in subsection (2) fails to comply with the requirement under that subsection, he shall commit an offence.

(4) Where a data controller fails to rectify, block, erase or destroy inaccurate personal data, a data subject may apply to the Commissioner to have such data rectified, blocked, erased or destroyed, as appropriate.

(5) Upon being satisfied by an application under subsection (4) that the personal data is incorrect, the Commissioner shall, where he is satisfied, direct the data controller to rectify, block, erase or destroy those data and any other personal data in respect of which he is the data controller.

(6) Where the Commissioner—

- (a) issues a direction under subsection (5); or
- (b) is satisfied on the application by an individual that personal data of which the individual is the data subject were inaccurate and have been rectified, blocked, erased or destroyed,

he may direct the data controller to notify third parties to whom the data have been disclosed, of the rectification, blocking, erasure or destruction.

(S. 44 came into operation on 16 February 2009.)

PART VII – EXEMPTIONS

45. National security

(1) 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.

(2) In any proceedings in which the non-application of any provision of this Act on grounds of national 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, shall be conclusive evidence of that fact.

(S. 45 came into operation on 16 February 2009.)

46. Crime and taxation

The processing of personal data for the purposes of—

- (a) the prevention or detection of crime;
- (b) the apprehension or prosecution of offenders; or
- (c) the assessment or collection of any tax, duty or imposition of a similar nature,

shall be exempt from—

- (i) the Second, Third, Fourth and Eighth Data Protection Principles;
- (ii) sections 23 to 26; and
- (iii) Part VI of this Act in respect of blocking personal data,

to the extent to which the application of such provisions would be likely to prejudice any of the matters specified in paragraphs (a) to (c).

(S. 46 came into operation on 16 February 2009.)

47. Health and social work

(1) A data controller shall be exempt from the application of section 41 where the personal data to which access is being sought relates to the physical or mental health of the data subject and the application of that section is likely to cause serious harm to the physical or mental health of the data subject or of any other person.

(2) The Prime Minister may, by notice in the *Gazette* or by regulations, waive the obligations imposed under section 41, on a public authority, voluntary organisations and such other similar body as may be prescribed, where that public authority, voluntary organisation or other body carries out social work in relation to a data subject or any other individual, and the application of that section is likely to prejudice the carrying out of the social work.

(S. 47 came into operation on 16 February 2009.)

48. Regulatory activities

The processing of personal data for the purpose of discharging any of the relevant functions—

- (a) designed for protecting members of the public against—
 - (i) financial loss due to dishonesty, malpractice or other serious improper conduct, or by the unfitness or incompetence of persons concerned in the provision of banking, insurance, investment or other financial services or in the management of bodies corporate;
 - (ii) financial loss due to the conduct of discharged or undischarged bankrupts; or
 - (iii) dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of persons authorised to carry on any profession or other activity;

- (b) conferred on the Bank of Mauritius, the Financial Services Commission and the Financial Intelligence Unit, by or under any enactment;
- (c) for protecting charitable trusts and other bodies involved in charitable work against misconduct or mismanagement in their administration;
- (d) for protecting the property of charitable trusts and other bodies specified in paragraph (c) from loss or misapplication;
- (e) for the recovery of the property of charitable trusts and other bodies specified in paragraph (c);
- (f) for securing the health, safety and welfare of persons at work;
- (g) for protecting persons, other than persons at work, against risk to health or safety arising out of or in connection with the actions of persons at work; or
- (h) designed for—
 - (i) protecting members of the public against conduct which adversely affects their interests, by persons carrying on a business;
 - (ii) regulating agreements or conduct which have as their object or effect the prevention, restriction or distortion of competition in connection with any commercial activity; or
 - (iii) regulating conduct on the part of one or more undertakings which amounts to the abuse of a dominant position in a market,

shall be exempt from the application of sections 23 to 26 to the extent that such an application would be likely to prejudice the proper discharge of such functions.

(S. 48 came into operation on 16 February 2009.)

49. Journalism, literature and art

(1) The processing of personal data for journalistic, literary and artistic purposes shall be exempt from the provisions specified in subsection (2) where—

- (a) such processing is undertaken with a view to the publication of any journalistic, literary or artistic material;
- (b) the data controller involved in such processing reasonably believes that the publication would be in the public interest; and
- (c) the data controller reasonably believes that compliance with any such provisions would be incompatible with such purposes.

(2) For the purposes of subsection (1), the processing of personal data shall be exempt from—

- (a) the Second, Third, Fifth and Eighth Data Protection Principles;

- (b) sections 23 to 27 and 32; and
- (c) Part VI in respect of blocking personal data.
(S. 49 came into operation on 16 February 2009.)

50. Research, history and statistics

(1) Subject to subsections (2), (4) and (5), personal data which are processed only for research, historical or statistical purposes shall be exempt from the Fifth Data Protection Principle.

(2) The exemption provided for under subsection (1) shall not be applicable where—

- (a) such personal data are not processed to support measures or decisions with respect to particular individuals; and
- (b) such personal data are processed in such a way that such processing would substantially damage or substantially distress any data subject or is likely to cause such damage or distress.

(3) For the purposes of—

- (a) the Second Data Protection Principle; and
- (b) sections 23 to 27,

further processing of personal data only for research, historical or statistical purposes shall not be regarded as incompatible with the purposes for which such data was obtained provided that the conditions under subsection (2) are satisfied.

(4) The personal data processed for the purposes specified in subsection (1) shall also be exempt from the provisions of Part VI where—

- (a) the conditions under subsection (2) (a) and (b) are satisfied; and
- (b) the results of the research or any resulting statistics are not made available in a form which identifies any of the data subjects concerned.

(S. 50 came into operation on 16 February 2009.)

51. Information available to public under an enactment

Where personal data consists of information which the data controller is obliged under an enactment to make available to the public, such data shall be exempt from—

- (a) the Second, Third, Fourth, Fifth and Eighth Data Protection Principles;
- (b) sections 23 to 29; and
- (c) Part VI in respect of blocking personal data.

(S. 51 came into operation on 16 February 2009.)

52. Disclosure required by law or in connection with legal proceedings

Personal data shall be exempt from—

- (a) the Second, Third, Fourth and Fifth Data Protection Principles;

- (b) sections 23 to 29; and
- (c) Part VI in respect of blocking personal data,

where—

- (i) the disclosure of such data is required under any enactment or by a Court order;
- (ii) the disclosure of such data is necessary for the purpose of, or in connection with, any on-going or prospective legal proceedings;
- (iii) the disclosure of such data is necessary for the purpose of obtaining legal advice; or
- (iv) the disclosure is otherwise necessary for the purpose of establishing, exercising or defending legal rights.

(S. 52 came into operation on 16 February 2009.)

53. Legal professional privilege

Personal data shall be exempt from—

- (a) the Second, Third, Fourth and Fifth Data Protection Principles; and
- (b) section 23,

where the data consist of information in respect of which a claim to legal professional privilege or confidentiality as between client and law practitioner could be maintained in legal proceedings, including prospective legal proceedings.

(S. 53 came into operation on 16 February 2009.)

54. Domestic purposes

Personal data processed by an individual shall be exempt from—

- (a) the Data Protection Principles; and
- (b) Part V and Part VI,

where such processing is only for the purposes of that individual's personal, family or household affairs or for recreational purposes.

(S. 54 came into operation on 16 February 2009.)

PART VIII – MISCELLANEOUS

55. Annual report

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

(2) Without limiting the generality of subsection (1), the report shall include—

- (a) a statement about the operation of approved and issued codes of practice;

- (b) any recommendations that the Commissioner thinks fit, in relation to compliance with this Act, and in particular the Data Protection Principles.

(3) 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 calendar year.

(S. 55 came into operation on 16 February 2009.)

56. Codes and guidelines

(1) The Commissioner may, for the purposes of this Act or any regulations made under this Act, issue or approve codes of practice, or issue guidelines.

(2) Before issuing or approving any code of practice, or issuing any guidelines, the Commissioner may consult such person or authority as he thinks fit.

(3) Any code of practice—

- (a) may be varied or revoked;
- (b) shall, where the code is approved under subsection (1), come into operation on a day specified by the Commissioner.

(4) The Commissioner shall keep a register of approved codes and guidelines which shall be available for public inspection.

(5) The Commissioner may, on payment of such fee as may be prescribed, provide copies of, or extracts from, the register specified in subsection (4).

(S. 56 came into operation on 16 February 2009.)

57. Service of notice

(1) Any notice served by the Commissioner on an individual under this Act may be served by—

- (a) delivering it to him;
- (b) sending it to him by registered post addressed to him at his usual or last known place of residence or business.

(2) Any notice served by the Commissioner on a body corporate under this Act may be served by—

- (a) sending it by post to the registered office of the body; or
- (b) addressing it to and leaving it at the registered office of the body.

continued on page D3 – 31

(3) Any notice served by the Commissioner on an unincorporated body of persons under this Act may be served by—

- (a) sending it by post to the place where it ordinarily carries out its activities; or
- (b) addressing it to and leaving it at the place where it ordinarily carries out its activities.

(S. 57 came into operation on 16 February 2009.)

58. Right of appeal

Any person aggrieved by a decision of the Commissioner in respect of the performance of his duties and powers under this Act shall have a right of appeal within 21 days from the date when the decision is made known to that person by the Tribunal.

(S. 58 came into operation on 16 February 2009.)

59. 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 section 59 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.

[S. 59 amended by s. 2 (p) of Act 1 of 2009 w.e.f. 22 May 2009.]

(S. 59 came into operation on 16 February 2009.)

60. Immunity and protection from liability

(1) Notwithstanding the Public Officers' Protection Act, where any action has been entered before a Court pursuant to any act done by any authorised officer in the execution of his duties under this Act or any regulations made under it, and it appears to the Court that there was reasonable cause to do such act, the Court shall so declare and thereafter the 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 or regulations made under it.

(S. 60 came into operation on 16 February 2009.)

61. Offences and penalties

(1) Any person who contravenes this Act shall commit an offence.

(2) Where no specific penalty is provided for an offence, the person shall, on conviction, be liable to a fine not exceeding 200,000 rupees and to imprisonment for a term not exceeding 5 years.

(S. 61 came into operation on 16 February 2009.)

62. Forfeiture

In addition to any penalty referred to in section 61, the Court may—

- (a) order the forfeiture of any equipment or any article used or connected in any way with the commission an offence;
- (b) order or prohibit the doing of any act to stop a continuing contravention.

(S. 62 came into operation on 16 February 2009.)

63. Prosecution and jurisdiction

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

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

(S. 63 came into operation on 16 February 2009.)

64. Consequential amendments

(1) The Criminal Code is amended by repealing section 300A.

(2) The Information and Communication Technologies Act is amended—

- (a) in section 2, by deleting the definitions of "code of practice" and "personal data";
- (b) by repealing section 33;
- (c) by repealing the Fourth Schedule.

(3) The National Computer Board Act is amended—

- (a) in section 2, by deleting the definitions of “computer service person”, “data”, “data user”, and “personal data”;
- (b) in section 4, by deleting paragraph (d); and
- (c) by deleting the First Schedule.

(S. 64 came into operation on 16 February 2009)

65. Regulations

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

(2) Regulations made under subsection (1) may provide—

- (a) for the requirements which are imposed on the data controller or data processor when processing data;
- (b) for the contents which a notification or application to a data controller or data processor should contain;
- (c) for the information to be provided to the data subject and how such information shall be provided;
- (d) for the levying of fees and taking of charges;
- (e) for the issuing and approval of codes and guidelines;
- (f) 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 2 years.

(3) The Prime Minister may, by regulations, amend the Schedules.

[S. 65 amended by s. 10 (h) of Act 14 of 2009 w.e.f. 30 July 2009.]

(S. 65 came into operation on 16 February 2009)

66. 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.

FIRST SCHEDULE

[Sections 2, 15 and 31]

DATA PROTECTION PRINCIPLES

First Principle

Personal data shall be processed fairly and lawfully.

Second Principle

Personal data shall be obtained only for any specified and lawful purpose, and shall not be further processed in any manner incompatible with that purpose.

Third Principle

Personal data shall be adequate, relevant and not excessive in relation to the purpose for which they are processed.

Fourth Principle

Personal data shall be accurate and, where necessary, kept up to date.

Fifth Principle

Personal data processed for any purpose shall not be kept longer than is necessary for that purpose or those purposes.

Sixth Principle

Personal data shall be processed in accordance with the rights of the data subjects under this Act.

Seventh Principle

Appropriate security and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Eighth Principle

Personal data shall not be transferred to another country, unless that country ensures an adequate level of protection for the rights of data subjects in relation to the processing of personal data.

[First Sch. amended by s. 10 (i) of Act 14 of 2009 w.e.f. 30 July 2009.]

SECOND SCHEDULE

[Section 6]

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 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
