Jurisdiction	Mauritius
Date	18 March 2022
Law Firm	Appleby
Title, Name	Malcolm Moller, Group Managing Partner Vaishali Damonaiko, Associate
Contact Information	+230 203 4300

Questionnaire

I. Law concerning protection of personal information

i. Does your country have a general law concerning the protection of personal information in the private sector at the present or in the near future?

Yes, the Data Protection Act 2017(as amended) in relation to personal data. 'Personal data' is any information relating to an individual data subject.

ii. Does your country have a general law concerning protection of personal information in the public sector at the present or in the near future?

Yes, the same laws as for private sector, as set out above, applies.

iii. Does your country have laws concerning protection of personal information which apply in individual sectors at the present or in the near future? (If yes, please describe outline.)

Yes, the same laws as for private sector, as set out above, applies.

Where all of the answers to the question of I.(i), (ii) and (iii) is "no", please skip to IV.

II. The basic information of the regulation concerning protection of personal information.

i. Please fill in the blanks below about the law concerning personal information mentioned at I.

The title of the law ：*Data Protection Act 2017 (DPA)*

① The definition of "Personal Information"	*any information relating to an individual data subject*
② The scope in which the law applies	*The Data Protection Act applies 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. *It 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.*
③ The territorial scope	*Applies in Mauritius only; no extraterritorial effect*

ii. If there are any special instructions about the laws, please describe them.

In addition to obtaining consent of the data subject and lawful processing as stated in this questionnaire, there are enhanced measures to process/collect ***special categories*** *of data which includes personal data pertaining to racial or ethnic origin, political opinion or adherence, religious or philosophical beliefs, membership of a trade union, physical or mental health or condition, sexual orientation, practices or preferences, genetic data or biometric data uniquely identifying the data subject, the commission or alleged commission of an offence by the data subject, any proceedings for an offence committed or alleged to have been committed by the data subject, 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.*

The additional measure are (a) 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; (b) the processing relates to personal data which are manifestly made public by the data subject; or (c) 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 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; (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.

III. OECD Privacy Principles

i. If there are any provision of law which embody each OECD Privacy Principle in your country, please describe the outlines.
https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

(a) Collection Limitation Principle

Collection of personal data: A data controller shall may only collect personal data where (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. (section 23(1) of DPA)

(b) Data Quality Principle

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.(section 21 of DPA)

(c) Purpose Specification Principle

Collection of personal data: Where a data 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 Data Protection 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 (section 23(2) of DPA).

(d) Use Limitation Principle

Unlawful disclosure of personal data: Any data 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.

Any data 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. Any person, except an employee or agent of a controller or processor and is acting within his mandate, 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 (section 42 of DPA).

(e) Security Safeguards Principle

Security of processing: A data controller or processor shall at the time of the determination of the means of processing and at the time of the processing, (a) implement appropriate security and organizational measures for the prevention of unauthorized access to, the alteration of, the disclosure of, the accidental

loss of and the destruction of the date in its control and 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. (section 31(1) of DPA)

(f) Openness Principle

Duties of controller: 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 the DPA (Section 22(1) of DPA).

(g) Individual Participation Principle

Rights of Data Subject:

- *Right of access (section 37 of DPA): Every controller shall, on the written request of a data subject provide, at reasonable intervals, without excessive delay and 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. However, 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.*
- *Automated individual decision making (section 38 of DPA): 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.*
- *Rectification, erasure or restriction of processing (section 38 of DPA): 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.*
- *Right to object: 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 (section 40 of DPA).*

(h) Accountability Principle

Breach of the above provisions shall be considered as an offence and on conviction, is punishable by fine and/or imprisonment.

ii. If there are any sectors in which any laws exclude the application of each OECD Privacy Principle, please describe the outline.

The following are exempted from the DPA:

1) where it constitutes a necessary and proportionate measure in a democratic society for – (a) subject to (c) below, 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; (e) the protection of a data subject or the rights and freedoms of others; or (f) issue of any licence, permit or authorisation during the COVID-19 period;

2) The processing of personal data for the purpose of historical, statistical or scientific research where the security and organisational measures specified in the DPA are implemented to protect the rights and freedoms of data subjects involved; and

3) Personal data 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.

(a) Collection Limitation Principle

(b) Data Quality Principle

(c) Purpose Specification Principle

(d) Use Limitation Principle

(e) Security Safeguards Principle

(f) Openness Principle

(g) Individual Participation Principle

(h) Accountability Principle

IV. Data Localization and Government Access

In your country, are there any systems having an impact on the rights of data subjects such as comprehensive government access to personal data or Data Localization? If yes, please describe them.

Please see advice at III (ii) above.

V. The Data Protection Authority

If there is the data protection authority, please write down the name and address of the authority

Data Protection Office
Level 5, SICOM Tower
Ebene Cyber City,
Ebene
Mauritius