Annex

The Data Protection Act of Mauritius

Mauritius enacted its first data protection legislation in 2004, then known as the Data Protection Act 2004. The DPA 2004 was proclaimed in 2009 to provide for the protection of the privacy rights of individuals in view of the developments in the techniques used to capture, transmit, manipulate, record or store data relating to individuals. The Data Protection Office was established in 2009 as a public statutory body under the DPA 2004.The office is now operating under the aegis of the Ministry of Information Technology, Communication and Innovation.

Since data protection is a dynamic field that is constantly challenged and influenced by advances in technology and innovation in business practices, consequently, the Data Protection Act 2004 was replaced by a new and improved legislation namely the Data Protection Act 2017[1] which came into force on 15 January 2018.

The preamble of the DPA 2017 stipulates the following:

"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"

The DPA 2017 has been brought at par with international best practices including the European Union General Data Protection Regulation 2016/679 (GDPR) and the Council of Europe Convention 108 and 108+.

The core principles of the Mauritius DPA are as follows:

a) DPA imposes several obligations on organisations for greater accountability and transparency, such as the appointment of a data protection officer, the notification of personal data breaches to the DPO as well as the notification to data subjects if the breach is likely to result in a high risk to the rights and freedoms of the data subjects, lawful processing of personal data, processing of special categories of personal data, processing personal data of child, the implementation of appropriate security measures, keeping a record of

1 https://dataprotection.govmu.org/Documents/DPA_2017_updated.pdf?csf=1&e=0rlrff

processing operations, evaluation of high-risk processing operations and the execution of data protection impact assessments, prior consultation and authorisation, registration of the organisation with the DPO, among others. Complying with the DPA, therefore, means meeting all the requirements stipulated in the DPA.

b) Data subjects have also been granted enhanced rights such as the right of access to his/her personal information, the right not to be subject to an automated individual decision making, the right to rectify, erase or restrict the processing of personal data and the right to object to the processing of his/her personal data.
c) The DPA provides the Data Protection Commissioner with enforcement powers to effectively exercise her functions. Failure to comply with the provisions of the DPA results in a breach which constitutes a criminal offence.
d) No exception is allowed to the DPA except where it constitutes a necessary and proportionate measure in a democratic society under limited circumstances as provided under section 44 of the DPA.

The rights and freedoms of individuals are taken into consideration in many sections of the DPA namely sections 26, 28, 34, 35, 36, 38, 40 and 44. The test of necessity and proportionality must be carried out for balancing the right to privacy with other rights and freedoms of the data subjects.

Mauritius has taken various international commitments on data protection such as being party to Convention 108 since 1 October 2016, the ratification of Convention 108+ on 04 September 2020 and the ratification of the Malabo Convention on 14 March 2018.

Our country is also party to the UN Declaration of Human Rights, the International Covenant on Civil and Political Rights and the Convention on Cybercrime (Budapest Convention).

Breaches of the DPA are criminal offences and penalties are provided in the Data Protection Act as described below:

Offences	Penalties
Section 6(5): Investigation of Complaints 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)	On conviction, be liable to a fine not exceeding 50,000 rupees and to imprisonment for a term not exceeding 2 years.
Section 7(2): Power to require information 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	On conviction, be liable to a fine not exceeding 50,000 rupees and to imprisonment for a term not exceeding 2 years.
Section 9(6): Enforcement notice Any person who, without reasonable excuse, fails or refuses to comply with an enforcement notice	On conviction, be liable to a fine not exceeding 50,000 rupees and to imprisonment for a term not exceeding 2 years.
Section 12: Obstruction of Commissioner or authorised officer Any person who, in relation to the exercise of a power conferred by section 11 (power of entry and search)- (a) obstructs or impedes the Commissioner or an authorised officer in the exercise of such power;	On conviction, be liable to a fine not exceeding 50,000 rupees and to imprisonment for a term not exceeding 2 years.

(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	
Section 15(3): Application for registration Any controller or processor who knowingly supplies any information, during registration, which is false or misleading in a material particular	On conviction, be liable to a fine not exceeding 100,000 rupees and to imprisonment for a term not exceeding 5 years.
Section 17(3): Change in particulars Any controller or processor who fails to notify a change in particulars within 14 days of the date of the change	On conviction, be liable to a fine not exceeding 50,000 rupees.
Section 28(2): Lawful processing Any person who processes personal data unlawfully	On conviction, be liable to a fine not exceeding 100,000 rupees and to imprisonment for a term not exceeding 5 years.
Section 29(3): Special categories of personal data Any person who processes special categories of personal data unlawfully	On conviction, be liable to a fine not exceeding 100,000 rupees and to imprisonment for a term not exceeding 5 years.
Section 43: Offence for which no specific penalty provided Any person who commits an offence under the Data Protection Act for which no	On conviction, be liable to a fine not exceeding 200,000 rupees and to

specific penalty is provided or who otherwise contravenes the Act	imprisonment for a term not exceeding 5 years. The Court may also order the forfeiture of any equipment or any article used or connected in any way with the commission of an offence or order or prohibit the doing of any act to stop a continuing contravention.
Section 49(3): Confidentiality and oath Any person who, without lawful excuse, divulges any confidential information obtained in the exercise of a power or in the performance of a duty under the Data Protection Act	On conviction, be liable to a fine not exceeding 50,000 rupees and to imprisonment for a term not exceeding 2 years.

The Data Protection Office

The Data Protection Office is an independent public office, established by the Data Protection Act, which ensures the consistent application of data protection rules in Mauritius.

The Data Protection Office became operational since 16 February 2009 and enforces the provisions of the Data Protection Act (DPA) 2017 (Annex 1). The office acts with complete independence and impartiality and is not subject to the control or direction of any other person or authority. The head of the office is known as the Data Protection Commissioner who is a barrister of not less than 5 years' standing as stipulated under the DPA.

The Data Protection Commissioner is assisted by such public officers as may be necessary. These public officers are under the administrative control of the Commissioner. The Commissioner may delegate any investigating or enforcement power conferred on her by the DPA to an officer of the office or to a police officer designated for that purpose by the Commissioner of Police.

The mission of the office is to safeguard the processing of personal data in the present age of information and communication. The office lays down an annual report of its activities before the National Assembly each year.