Republic of Mauritius

Annual Report
of the
Data Protection Office

Prime Minister's Office
Year 2009

No. 4 of 2010

Annual Report

of the

Data Protection Office

Vision of the Data Protection Office

- A society where Data Protection is understood and practiced by all.
- The right to privacy and data protection is primordial to the sanctity of any modern democracy.
- The adoption of clear procedures for the collection and use of personal data in a responsible, secure, fair and lawful manner, by all data controllers and data processors.

Contents

Forward

Data protection has substantially and positively grown in stature and influence since the institution of the Data Protection Office. Data protection is fundamental to people's lives and to the good business reputations of public and private organisations. It has been and still is very challenging for the Data Protection Office to infiltrate data protection and make it a firmly-established part of the fabric of Mauritian life. However, the response to the challenge has been very encouraging from the diverse sectors.

Data protection underpins modern democracy and the fundamental liberties entrenched in our Constitution and is also pivotal to a trusted relationship between the state and the citizen.

Personal information, especially sensitive personal data, can be the greatest asset of an organisation as well as the most dangerous liability, if not handled properly. Information management demands clear lines of accountability and responsibility, coherent policies and procedures, rigorous training and regular checks on our institutions.

The privacy of personal information has become a global imperative for governments, commerce and civil society over the past decade or so. We have all reaped tremendous benefits from the technological advances that have put more computing power in our hands year after year, increasing our abilities to communicate, learn, share, and produce. To preserve these benefits and to promote the wide-spread adoption and use of new technologies generally, we must embed trust in the relationships created by these technologies by promoting and ensuring the privacy of personal information.

Respecting privacy is thus far more than a moral imperative - it also offers substantial dividends. For businesses, the "privacy payoff" may come in the guise of enhanced credibility, reduced legal liabilities, more efficient operations, and above all, improved customer confidence and trust.

In addition to performing its statutory functions, this Office is committed to provide the best possible service to help organisations and the public at large to understand their data protection rights and obligations. It is the wish of this Office that this First Annual Report will contribute towards a better understanding and knowledge of data protection for the benefit of one and all.

Drudeisha Madhub (Barrister-at-Law)
Data Protection Commissioner

Introduction

- The Data Protection Act 2004 was proclaimed in its entirety on the 16th of February 2009, except for section 17. In addition, the Data Protection Regulations 2009 (GN 22/09) were enacted in order to cater for the registration fees for data controllers, other prescribed fees, the registration form for data controllers and the request for access to personal data form which represents the form to be used by data subjects who are living individuals, for requesting access to their personal data from data controllers.

- Data Protection physically came to life in Mauritius through the National Information, Communication and Telecommunication Strategic Plan 2007-2011 wherein the setting up of the Data Protection Office was recommended.

- The Data Protection Act 2004 was updated to secure better chances of accreditation with the European Union for Mauritius to be recognised as an adequate country in data protection to facilitate the transfers of personal data from the European Union to Mauritius and thus attract more investment in mainly the information technology and business processing outsourcing sectors of the Mauritian economy.

- The Data Protection Act 2004 gives individuals rights to protect them against data protection breaches, and creates obligations for those keeping personal information. Under the Act, individuals have the right to be informed of any data processing activity which relate to them as data subjects.

- *Data* is defined in the Act as "information in a form which is capable of being processed by means of equipment operating automatically in response to instructions given for that purpose; and is recorded with the intent of it being processed by such equipment; or is recorded as part of a relevant filing system or intended to be part of a relevant filing system."

- *Personal data* is defined in the Act as "data which relate to an individual who can be identified from those data; or 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."

- *Data Controller* is defined in the Act as "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 Processor* is defined in the Act as "a person, other than an employee of the data controller, who processes the data on behalf of the data controller."

- As per section 3 of the Data Protection Act, data protection concerns both the state and private stakeholders. Thus, a data controller or a data processor may either be a public or a private institution. The Data Protection Act will apply to a data controller: (a) who is established in Mauritius; and (b) who is not established in Mauritius, but uses equipment in Mauritius for processing data for other purposes than mere transit. A data controller is deemed to be established when he is a resident in Mauritius and/or carries out data processing activities through an office, branch or agency in Mauritius. When not established in Mauritius, a data controller must nominate a representative in Mauritius.

- The data protection agenda ranges from biometrics to simple personal details kept or processed in a structured filing system or on a computer such as names, addresses and identity numbers as it concerns all information directly or indirectly related to a living individual who are termed data subjects under the Data Protection Act.

- The role of the Data Protection Office is to ensure that clear procedures on collection and use of personal data in a responsible, secure, fair and lawful manner are adopted with a view to protecting personal data.

- The principal purpose for registration and the creation of a public register is transparency or openness. The public should know or should be able to find out who is carrying out processing of their personal data and any other information about the processing, such as, for what purposes the processing are being carried out.

- Registration serves two-folded interests, it serves the interests of data controllers in providing a mechanism to publicise details of their processing activities and also serves the interests of data subjects in assisting them to understand how personal data are being processed by data controllers.

- This Report covers the period February to December 2009.

The Data Protection Office

The Data Protection Office which is headed by a Data Protection Commissioner is located on the 4th floor, Emmanuel Anquetil Building, Port-Louis.

Phone: 201 36 04
Fax: 201 39 76
Website: http://dataprotection.gov.mu
Email: pmo-dpo@mail.gov.mu

The Data Protection Act

Registration of Data Controllers and Data Processors

Section 33 of the Data Protection Act provides that every data controller and data processor must before keeping or processing personal data or sensitive personal data, register himself with the Commissioner upon the payment of the relevant fees enacted under the Data Protection Regulations. Failure to register or to renew registration within three months before the date of expiry of registration, on an annual basis, is an offence under the Act and the regulations.

Obligations of Data Controllers and Data Processors

The data protection principles represent the founding milestones of personal data protection law which are to be cautiously and meticulously followed and implemented by all sectors. In common parlance, they are the good practices to be followed by one and all.

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 the 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.

Rights of data subjects

In accordance with section 41 of the Act, a data controller must upon the written request of a data subject inform the data subject on any personal data kept by him (data controller); the purpose/s for keeping the data; and the third parties to whom the data may be disclosed by the data controller.

A data controller may refuse to comply with the request if he is not provided with such information as he may reasonably require to determine the identity of the data subject and to locate the information being requested.

Where a data controller cannot comply with the request without disclosing the personal data to another person, he may refuse the request unless the other person is agreeable to his personal data being disclosed to the person making the request or he obtains the approval of the Commissioner.

Data controllers do not need to comply with a request where they have already complied with an identical or similar request by the same individual unless a reasonable interval has elapsed between compliance with the previous request and the making of the current request.

Where the information sought by the data subject relates to the physical or mental health of the individual, the data controller may be exempt from the application of section 41 where he establishes that the application of section 41 is likely to cause serious harm to the physical or mental health of the data subject or to any other person.

Exemptions under the Act

There is no exemption from registration catered for in the law, except for: (a) personal data which is required for national security purposes; and (b) personal data processed by an individual for personal, family, household or recreational purposes.

Other listed exemptions such as crime and taxation, health and social work, regulatory activities, journalism, literature art, research, history and statistics, information available to the public under an enactment, disclosure required by the law or in connection with legal proceedings, and legal professional privilege, are exempt only from certain varying sections of the Act.

Data controllers should further exercise caution when relying upon an exemption under the Act and should not regard it as providing automatic or blanket exclusion from the application of the provisions of the Act.

Activities carried out during year 2009

Registration of data controllers was initiated in 2009. A Data Protection Register is kept by the office as per the requisites laid down in section 33 of the Act.

Guidelines and sectoral codes of practice, as per the demands and the needs of the sectors were developed and assistance was provided to the organisations concerned to respond appropriately to data security breaches by adopting the relevant guidelines.

To-date, five guidelines have been issued to provide a detailed understanding of the provisions of the Data Protection Act. These guidelines are as follows:

(a) A practical guide for data controllers and data processors which is a comprehensive document on the obligations of data controllers and data processors under the Data Protection Act, enumerating all the legal and practical steps to be followed by them in implementing the legislation.

(b) Registration Classification and Guidance Notes for Application of Data Controllers and Data Processors have been issued to facilitate the task of data controllers and data processors for registration.

(c) A Guide on Data Protection Rights which highlights all the rights of the data subjects, i.e, living individuals, who are the subjects of personal data.

(d) Guidelines for Handling Privacy Breaches to assist public and private sector organisations whenever a privacy breach occurs.

(e) Guidelines to regulate the processing of personal data by video surveillance systems.

A Code of Practice has also been developed and which has come into operation on the 24th of April 2009 to be implemented by the Police Force whilst using Closed Circuit Television Systems to monitor road traffic, in compliance with section 56 of the Data Protection Act

A leaflet on data protection was distributed to individuals or organisations concerned to sensitise them on their respective rights and obligations under the Data Protection Act. Communiques were also issued on television and the press for the registration of data controllers.

A Self-Assessment Questionnaire to be filled in by data controllers and processors prior to security checks being conducted by the authorised officers of the office and a Data Protection Audit Questionnaire before effecting compliance audits have also been developed. Both documents are posted on the homepage of the website in order to familiarise data controllers and processors on the implementation of data protection in their respective organisations.

Diverse sensitisation campaigns to simplify the understanding of the legal provisions of the Data Protection Act with the assistance of organisations such as the National Computer Board, Mauritius Bankers' Association, Outsourcing Telecommunications Association of Mauritius, Ministry of Information and Technology, University of Technology of Mauritius, Legal Department of the University of Mauritius, National Security Advisor's Office, Mauritius Employers' Federation and Board of Investment have been organised.

The website of the office (http://dataprotection.gov.mu) was designed and posted on the government portal to assist the various sectors of the economy as well as the public to access all relevant information on the Office. To facilitate the task of data controllers for registration, this Office has posted a specimen registration form for data controllers on the homepage of the website apart from drafting guidelines for the filling in of registration forms also available on the website. The list of registered data controllers is also posted on the website.

A "teens corner" found on the website, has further been developed in order to sensitise young people on the pros and cons of social networking sites.

A large number of queries were received by the public on a very broad range of issues, from access rights to registration obligations. Emails were the medium for the most common source of queries with a smaller number of queries received by post. Most of the queries were attended to. The Data Protection Office is continuing its efforts to use innovative tools to reach more people and to inform them of their rights.

As regards the potential data controllers who are not yet registered with the office, efforts are on-going to sensitise them on their statutory obligations to register.

Designed & Printed by the Government Printing Department