The Data Protection Legislation aims to ensure that personal information in the custody, or under the control, of an organization, whether public or private, shall not be disclosed, processed or used other than for the purpose for which it was collected, except with the consent of the individual and where exemptions are clearly defined.

The Data Protection Bill thus creates binding obligations with respect to the:
- collection
- use, and
- disclosure
of personal information, as well as setting out access rights.

The Data Protection Bill seeks to protect individuals by requiring organizations to:
- notify persons as to the purpose for collecting their personal information, and
- follow certain policies and practices for sharing such information.

There are several reasons for having legislation to regulate the collection and use of personal data:
- Technology now makes it easy to gather, retrieve, disseminate and manipulate huge amounts of personal data. This has given rise to concerns that the privacy of individuals can be easily compromised.

Lack of security and privacy is often cited as the main reason for the slow growth of electronic transactions, (and thus, e-commerce and e-government). Several international surveys showed it to be the number one concern of businesses in doing business.
The legislation may thus promote e-government and e-commerce in Mauritius as the availability of legal protection of personal data will encourage consumers and businesses to transact online.
The Data Protection Act complements the objectives of the Electronic Transactions Act as it:

- Protects the individual's right to privacy thus giving them greater confidence in the use of e-commerce and e-Government.
- Provides enhanced protection for the physical and electronic security of personal information.

Value-added benefit of legislation

Ensures personal information is used correctly, that the information is accurate and limits access to the information to only those with a legitimate right to the information.

Ensures successful facilitation of trading relations with international partners that have similar legislation.

Within the completed Economic Partnership Agreement, maintaining comparable standards is cited as important for the ability to carry on trade with European Union member countries.

Data protection legislation is also a prerequisite for attracting certain off-shore investment services.

Documents consulted

- Data Protection Directive.

The basic principles to be included are the following:

- **the purpose limitation principle** - data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer. The only exemptions to this rule would be those necessary in a democratic society on one of the grounds listed in Article 13 of the directive.
- **the data quality and proportionality principle** - data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed.

WP 12 Provisions

WP 12: On the issue of what constitutes adequate protection, two basic elements must be assessed: the **content of the applicable rules and the means for ensuring their effective implementation**. In assessing compliance with these elements, it is important to have a basic list of minimum requirements for ensuring adequacy.
Examples of additional principles to be applied to specific types of processing are:

- sensitive data - where ‘sensitive’ categories of data are involved (those listed in article 8 of the directive), additional safeguards should be in place, such as a requirement that the data subject gives his/her explicit consent for the processing.
- direct marketing - where data are transferred for the purposes of direct marketing, the data subject should be able to ‘opt-out’ from having his/her data used for such purposes at any stage.
- automated individual decision - where the purpose of the transfer is the taking of an automated decision in the sense of Article 15 of the directive, the individual should have the right to know the logic involved in this decision, and other measures should be taken to safeguard the individual’s legitimate interest.

Weaknesses of the Directive continued...

- The measures aimed at providing transparency of data processing through better information and notification are inconsistent and ineffective.
- The obligation on data controllers to provide information to data subjects, evidenced via privacy notices, privacy policies or consent notices connotes active communication of the information as opposed to making sure that the information can be found, e.g. on a website. Such an active means of communication may be difficult to apply in practice given transformation in social networking. Additionally, consumers opine that privacy policies are not necessarily written in a consumer-friendly manner and fail to assist them in understanding their rights.
Weaknesses of the Directive continued...
- The notification obligation of Article 18 of the Directive requires a data controller to notify the relevant national supervisory authority before carrying out automatic processing, with allowances for exemptions and simplifications where rights and freedoms of the data subject are unlikely to be adversely impacted. The purpose is to increase awareness and improve monitoring. The report notes that this notification requirement is a weakness of the regime and inhibits harmonisation. It is outdated as processing personal data is no longer a static, localised process, but is ubiquitous. There are better ways to ensure transparency.

Weaknesses of the Directive continued...
- The rules on data export and transfer to third countries are outmoded - Interviewees expressed the opinion that specific rules for transferring data to a third country were not appropriate in an era of globalisation, with practical problems for protecting the data of European citizens arising due to the sheer quantities of personal information transferred. The adequacy rule was also thought to be highly restrictive and polarizing, resulting in a mechanism where only countries that follow the Directive strictly are considered to have an adequate protection regime, in effect creating not an adequacy test, but an equivalence (i.e. transposition) test. The perception is that the adequacy review is merely a review of paper and policy, rather than a serious investigation of how personal data is protected.

Weaknesses of the Directive continued...
- The tools providing for transfer of data to third countries are cumbersome - The RAND report indicates that in an increasingly global, networked environment, the Directive as it stands will not suffice in the long-term. The widely applauded principles of the Directive will remain as a useful front-end, yet will need to be adapted to a harms-based back-end in due course, in order to be able to cope with the challenges of globalisation and flows of personal data.

CONCLUSION
- The review notes variances in transposing the requirements of the Directive and the outmoded nature of the Directive given the increase in data processing due to technological advances. Despite recommendations for amending the Directive to address its inefficiencies, adequacy requirements must still be assessed in light of existing provisions.
Amendments to The Data Protection Act

- Formal request made to Data Protection Unit of the Directorate-General Justice of the European Commission
- Report: Analysis of Adequacy of the Protection of personal Data in Mauritius aimed to provide the European Commission with information of regime in Mauritius in order to determine if the law provides an adequate level of protection

Right to object to be inserted:
- An individual has the right to object, for legitimate reasons, to his personal data being processed.
- The data subject has no right to object where the processing is under a legal obligation, or where the right to object is excluded by an explicit provision of the decision authorising the processing.

- Insertion of some e-government provisions eg
  - A certified copy of, or of an extract from, any entry in the register may be obtained from the commissioner in paper or electronic format and the electronic format shall be as legally valid as the paper format.

- Certain definitions to correspond to those in directive eg personal data, processing, individual
- Provision on Processing of sensitive personal data, Transfer of personal data and Exemptions to be amended to correspond to those in directive
- Removal of requirement for renewal
- §2 of the DPA on ‘Information available to the public’ is not compliant with the Directive and is to be repealed

Presented by: Tira Greene
E-mail: tiragreene@yahoo.com