Data Protection Office

DATA PROTECTION ACCREDITATION FOR MAURITIUS

November 24, 2011
Port Louis, Mauritius

DATA PROTECTION ACCREDITATION FOR MAURITIUS

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.

DATA PROTECTION ACCREDITATION FOR MAURITIUS

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.

DATA PROTECTION ACCREDITATION FOR MAURITIUS

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.

DATA PROTECTION ACCREDITATION FOR MAURITIUS

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.

DATA PROTECTION ACCREDITATION FOR MAURITIUS

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.

DATA PROTECTION ACCREDITATION FOR MAURITIUS

Value-added benefit of legislation

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.

DATA PROTECTION ACCREDITATION FOR MAURITIUS

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.

DATA PROTECTION ACCREDITATION FOR MAURITIUS

- ❖ 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.

DATA PROTECTION ACCREDITATION FOR MAURITIUS

Documents consulted

- Data Protection Directive.
- Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Working Document on the "Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive" (WP 12), Adopted by the Working Party on 24 July 1998.
- First Report from the Commission on Implementation of the Data Protection Directive (COM (2003) 265 final).
- Working Document on the Processing of Personal Data Relating to Health in Electronic Health Records (EHR) Adopted on 15 February 2007.
- Review of the Data Protection Directive, RAND Report to the Information Commissioner's Office 2009.

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

WP 12 Provisions – *(i) Content principles*

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

- **the transparency principle** - individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country, and other information insofar as this is necessary to ensure fairness. The only exemptions permitted should be in line with Articles 11(2)3 and 13 of the directive.
- **the security principle** - technical and organisational security measures should be taken by the data controller that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller.

WP 12 Provisions

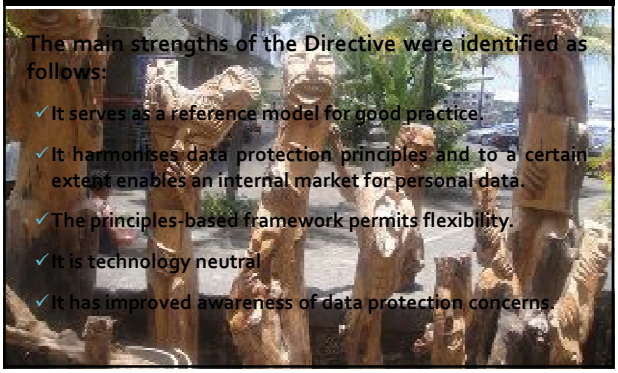
- **the rights of access, rectification and opposition** - the data subject should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her. The only exemptions to these rights should be in line with Article 13 of the directive.
- **restrictions on onward transfers** - further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection. The only exceptions permitted should be in line with Article 26(1) of the directive.

WP 12 Provisions

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 directive4), 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.

RAND REVIEW OF THE EUROPEAN DATA PROTECTION DIRECTIVE



RAND REVIEW OF THE EUROPEAN DATA PROTECTION DIRECTIVE

The main weaknesses of the Directive were identified as follows:

- **The link between the concept of personal data and real privacy risks is unclear** - The Directive fails to show a real link between privacy protection and data protection, all acts of personal data processing as covered by the Directive do not have a clear or noticeable privacy impact. The Directive connotes a fundamental rights interpretation of data protection, where personal data is deemed inherently worthy of protection.

RAND REVIEW OF THE EUROPEAN DATA PROTECTION DIRECTIVE

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.

RAND REVIEW OF THE EUROPEAN DATA PROTECTION DIRECTIVE

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 outmoded as processing personal data is no longer a static, localised process, but is ubiquitous. There are better ways to ensure transparency.

RAND REVIEW OF THE EUROPEAN DATA PROTECTION DIRECTIVE

Weaknesses of the Directive continued…

- There are divergences in EU implementation.
- The purpose of the notification process as a register of data controllers was also questioned, with registers viewed as indirect forms of taxation or only useful to lawyers conducting due diligence exercises, with little use for consumers.

RAND REVIEW OF THE EUROPEAN DATA PROTECTION DIRECTIVE

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.

RAND REVIEW OF THE EUROPEAN DATA PROTECTION DIRECTIVE

Weaknesses of the Directive continued…

- **The tools providing for transfer of data to third countries are cumbersome** – Alternative mechanisms for data transfer, which require data controllers to assume direct responsibility for ensuring the security of the transfer, in particular Binding Corporate Rules (BCRs) and Standard Contractual Clauses (SCCs), were perceived as a much more positive approach to transfers to third countries. However, several issues remain unresolved such as the processes for accepting standard clauses. It was thought that (a) harmonising the procedures for approving contractual clauses, and (b) make mutual acceptance mandatory, so that approval by the DPA in one Member State would make further steps in other Member States unnecessary would allow for more efficient use of the resources of data protection authorities.

RAND REVIEW OF THE EUROPEAN DATA PROTECTION DIRECTIVE

Weaknesses of the Directive continued…

- **The definition of entities involved in processing and managing personal data is simplistic and static** - The relationship between processor and data controller envisaged in the Directive is outdated in a networked society and does not adequately cover the variety of entities involved in the processing of personal data. Practical difficulties exist in determining when a processor becomes a controller or vice versa, especially online where visiting a website might result in cookies being sent from a number of sources located in various jurisdictions. Business processes in off-shoring, outsourcing, sub-processing and onward transfer have created the need for companies to conclude contracts among themselves and with sub-contractors involved in processing, in complying with the law. However, reviewing each contract is unnecessarily burdensome.

RAND REVIEW OF THE EUROPEAN DATA PROTECTION DIRECTIVE

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 supported with 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 out-moded 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

Amendments to The Data Protection Act

- 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
- 51 of the DPA on 'Information available to the public' is not compliant with the Directive and is to be repealed

Amendments to The Data Protection Act

- 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.

Thank You

Presented by: Tira Greene

E-mail: tiragreene@yahoo.com