# Assessment Report on Privacy and Data Protection

**Presentation at the**

**First Consultation Workshop for**

**Working Group 1 – ITU-EC HIPCAR Project**

Saint Lucia, 8-12 March 2010

# Objective

- This presentation seeks to:
  - highlight the major trends found in established Privacy and Data Protection frameworks in the international arena to determine best practice;
  - Provide initial assessments of regional Privacy and Data Protection frameworks against the defined best practice.

# Overview

- Personal Privacy is considered a tenet of the UN Charter of Human Rights
- Frameworks for protection of personal are not new, however there has been renewed focus on the protection of information collected by Governments since the late 1970's
- The OECD adopted their "Guidelines for Protection of Privacy in Transborder Flows" in 1980
  - The resultant framework is considered a foundation of contemporary data protection frameworks in force up to today!

# Overview

- The subsequent ubiquity of information processing systems within the Public and Private Sectors merited the development of guidelines by a broader set of stakeholders
- In 1990, the UN adopted “Guidelines for Computerised Personal Data Files”
- These guidelines provided minimum guarantees to be included in national legislation
  - requiring much of the OECD adopted requirements even in instances where there were no trans-border data transfers!
- Together, the UN and OECD guidelines form the basis of most international Data Protection frameworks

# Key Principles of Data Protection

| OECD "Guidelines" | UN "*Guidelines*" |
|---|---|
| 1. | 1. Lawfulness and fairness |
| 2. Data Quality | 2. Accuracy |
| 3. Purpose Specification | 3. Purpose-specification |
| 4. Use Limitation | 4. Interested-person access |
| 5. Security Safeguards | 5. Non-discrimination |
| 6. Openness | 6. Exception Making |
| 7. Individual Participation | 7. Security |
| 8. Accountability | 8. Supervision and sanctions |
| | 9. Transborder data flows |
| | 10. Field of application |

# Developing an analytical benchmark

The Report identifies 6 areas of consideration which together encapsulate all principles:

1. Legal Mandate
2. Institutional Framework
3. Regulatory Empowerment
4. Collection of Personal Information
5. Storage and Use of Personal Information
6. Disclosure of Personal Information

# Legal Mandate: Key Questions

- Is there a clear legal mandate protecting privacy and personal information?
- Is the framework applicable to both the public and private sectors?
- Does the framework clearly outline the condition that personal information should only be collected with the consent of the subject of that personal information?
- Does the framework limit the processing of ‘sensitive information’?
- Does the framework outline conditions of exemptions from the guidelines therein?

# Institutional Framework: Key questions

- Does the framework make it clear who is responsible for ensuring compliance to the obligations outlined?
- Is the oversight body a distinct legal person, who takes direction from no other person in the execution of his duty?
- Is the oversight body independent of the persons who would be responsible for the collection and use of personal information, including Government and private sector interests?
- Is this oversight body afforded powers and privileges necessary to support its investigative functions?

# Regulatory Empowerment: Key questions

- Does the framework clearly underscore the nature of the interaction between these persons and the oversight body?
- Does the framework provide for cooperation in the instance of investigation by the oversight body?
- Does the framework provide for enforcement actions to be taken against errant collectors of information?

# Collection of Personal Information: Key questions

- Does the framework provide for the data subject's notification of purpose for collection by the collecting party before collection?
- Does the framework oblige the collector of information to limit the type of data collected for a given purpose?
- Does the framework limit the collecting party's retention of information to that period for which it is necessary?
- Does the framework recognize the particular demands for information protection in the health sector with regard to data collection

# Storage and Use of Information: Key questions

- Does the framework limit the use of data collected to that purpose given at the notification of the data subject?
- Does the framework oblige the collecting agency to ensure correctness of information?
- Does the framework provide for the subject's validation of the information stored?
- Does the framework oblige the collecting agency to safeguard the information collected?
- Does the framework provide for the oversight body approving particular types of information processing

# Disclosure of Information: Key questions

- Does the framework limit the disclosure of the information stored unless prior consent is gained from the data subject?
- Does the framework allow for exemptions for reasons of national security, health and provision of justice?
- Does the framework limit the transfer of information to a jurisdiction without like protections for personal information?

# Summary of findings

| Country/ Region | 1. Legal Mandate | 2. Institutional Framework | 3. Regulatory Empowerment |
|---|---|---|---|
| Antigua & Barbuda | NONE | NONE | NONE |
| Bahamas | **GOOD** | **GOOD** | **GOOD** |
| Barbados | POOR | NONE | NONE |
| Belize | NONE | NONE | NONE |
| Dominica | NONE | NONE | NONE |
| Dominican Republic | NONE | NONE | NONE |
| Grenada | NONE | NONE | NONE |
| Guyana | NONE | NONE | NONE |
| Haiti | NONE | NONE | NONE |
| Jamaica | NONE | NONE | NONE |
| St. Kitts & Nevis | NONE | NONE | NONE |
| St. Lucia* | (GOOD) | (GOOD) | (GOOD) |
| St. Vincent & the Grenadines | FAIR | **POOR** | FAIR |
| Suriname | NONE | NONE | NONE |
| Trinidad & Tobago* | (GOOD) | (GOOD/ FAIR_ | (GOOD) |

# Summary of findings (cont'd)

| Country/ Region | 4. Collection of Personal Information | 5. Storage and Use of Information | 6. Disclosure of Information |
|---|---|---|---|
| Antigua & Barbuda | NONE | NONE | NONE |
| Bahamas | **GOOD** | **GOOD** | **GOOD** |
| Barbados | NONE | NONE | POOR |
| Belize | NONE | NONE | NONE |
| Dominica | NONE | NONE | NONE |
| Dominican Republic | NONE | NONE | NONE |
| Grenada | NONE | NONE | NONE |
| Guyana | NONE | NONE | NONE |
| Haiti | NONE | NONE | NONE |
| Jamaica | NONE | NONE | NONE |
| St. Kitts & Nevis | NONE | NONE | NONE |
| St. Lucia* | (GOOD) | (GOOD) | (GOOD) |
| St. Vincent & the Grenadines | **GOOD** | FAIR | FAIR |
| Suriname | NONE | NONE | NONE |
| Trinidad & Tobago* | (GOOD) | (GOOD) | (GOOD) |

# Recommendations

- Harmonisation is needed in the appropriate locus of the Data Commissioner with respect to the Political Executive and the Private Sector
  - Associated with this decision would be the powers of investigation and enforcement associated with the functions of the Data Commissioner
- Harmonisation and consensus required on what is considered a “public authority”
- Harmonisation of the approach of recognising Data Controllers
  - Should there be a registration of data controllers, or should there be a general applicability approach

# THANK YOU

**Kwesi PRESCOD**
***Prescod Associates & Co.***
***PO Box 3228***
***Petit Valley***
***TRINIDAD & TOBAGO***

*Website: www.prescodassociates.com*
*e-mail: kwesiprescod@prescodassociates.com*
*Tel: + 1 868 633 2951*
*Mobile: + 1 868 688 4380*
*Fax: + 1 868 632 3606*