Establishment of Harmonized Policies for the ICT Market in the ACP Countries

Privacy and Data Protection:

Assessment Report

HIPCAR

Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean

Disclaimer

This document has been produced with the financial assistance of the European Union. The views expressed herein do not necessarily reflect the views of the European Union.

The designations employed and the presentation of material, including maps, do not imply the expression of any opinion whatsoever on the part of ITU concerning the legal status of any country, territory, city or area, or concerning the delimitations of its frontiers or boundaries. The mention of specific companies or of certain products does not imply that they are endorsed or recommended by ITU in preference to others of a similar nature that are not mentioned. This report has not been through editorial revision.

Please consider the environment before printing this report.

Foreword

Brahima Sanou
BDT, Director

Acknowledgements

The present document represents an achievement of the regional activities carried out under the HIPCAR project "Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures", officially launched in Grenada in December 2008. It is a companion document to the Model Policy Guidelines and Legislative Texts on this HIPCAR area of work[1].

In response to both the challenges and the opportunities from information and communication technologies' (ICTs) contribution to political, social, economic and environmental development, the International Telecommunication Union (ITU) and the European Commission (EC) joined forces and signed an agreement aimed at providing "*Support for the Establishment of Harmonized Policies for the ICT market in the ACP*", as a component of the programme "ACP-Information and Communication Technologies (@CP-ICT)" within the framework of the 9th European Development Fund (EDF), i.e., ITU-EC-ACP project.

This global ITU-EC-ACP project is being implemented through three separate sub-projects customized to the specific needs of each region: the Caribbean (HIPCAR), sub-Saharan Africa (HIPSSA) and the Pacific Island Countries (ICB4PAC).

The HIPCAR Steering Committee – chaired by the Caribbean Telecommunications Union (CTU) – provided guidance and support to a team of consultants including Ms. Karen Stephen-Dalton and Mr. Kwesi Prescod, who prepared the initial draft documents. The documents were then reviewed, finalized and adopted by broad consensus by the participants at the First Consultation Workshop for HIPCAR's Working Group on ICT Policy and Legislative Framework on Information Society Issues, held in Saint Lucia on 8-12 March 2010. Based on the assessment report, Model Policy Guidelines and Legislative Texts were developed, reviewed and adopted by broad consensus by the participants at the Second Consultation Workshop held in Barbados on 23-26 August 2010.

ITU would like to especially thank the workshop delegates from the Caribbean ICT and telecommunications ministries and regulators as well as their counterparts in the ministries of justice and legal affairs, academia, civil society, operators, and regional organizations, for their hard work and commitment in producing the contents of the HIPCAR model texts. The contributions from the Caribbean Community Secretariat (CARICOM) and the Caribbean Telecommunications Union (CTU) are also gratefully acknowledged.

Without the active involvement of all of these stakeholders, it would have been impossible to produce a document such as this, reflecting the overall requirements and conditions of the Caribbean region while also representing international best practice.

The activities have been implemented by Ms Kerstin Ludwig, responsible for the coordination of activities in the Caribbean (HIPCAR Project Coordinator), and Mr Sandro Bazzanella, responsible for the management of the whole project covering sub-Saharan Africa, the Caribbean and the Pacific (ITU-EC-ACP Project Manager) with the overall support of Ms Nicole Darmanie, HIPCAR Project Assistant, and of Ms Silvia Villar, ITU-EC-ACP Project Assistant. The work was carried under the overall direction of Mr Cosmas Zavazava, Chief, Project Support and Knowledge Management (PKM) Department. The document has further benefited from comments of the ITU Telecommunication Development Bureau's (BDT) ICT Applications and Cybersecurity Division (CYB), and Regulatory and Market Environment Division (RME). Support was provided by Mr. Philip Cross, ITU Area Representative for the Caribbean. The team at ITU's Publication Composition Service was responsible for its publication.

[1] HIPCAR Model Policy Guidelines and Legislative Texts, including implementation methodology, are available at www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html

Table of Contents

Page

Section I:
Summary and Introduction

1.1 Introduction

Privacy is described as one of the most basic human rights protected in major international human rights instruments[2] and one of the building blocks of trust in the security and confidentiality of communications and sensitive data- a trust that is essential to e-commerce and full realization of the potential benefit of the information society.[3]

The concept of privacy embodies a number of aspects including anonymity, solitude and confidentiality so that a person's right to privacy is thought to include:

- the right to enjoy a certain amount of personal life free from unwanted interruptions or intrusions;
- the right to communicate with other people without unwanted surveillance;
- the right to control access to information about one's personal life.

The converged environment and increasing sophistication of information and communications technology has enabled the worldwide transmission of personal information, making it easier to access, collect and share and transmit personal information in particular, via the internet, in seconds across borders and from anywhere in the world. While advances information and communications technology offer great potential for e-commerce, including increased choice for consumers, expansion of markets, innovation, productivity and education, there is a concomitant heretofore unequaled potential for the intrusion and subversion of individual's personal communications and privacy. Further, by the nature of technological systems, very often these intrusive, subversive activities are undetected by the targeted persons.

It is in this context, that the increase in the use of the Internet and other forms of information and communications technology as tools for conducting business, whether nationally, regionally and internationally, raises significant questions and concerns for service providers, businesses and consumers regarding the protection of private and/ or personal information that are transmitted through these means.

Further, policy makers are provided with challenges with respect to two goals which appear to be disparate:

(i) the creation of an environment in which citizens rights are protected, and

(ii) the avoidance of unnecessary restrictions on the transmission of information across borders that could inhibit the growth of electronic commerce.

Increasingly consumers' privacy is threatened by new information and communications technologies and the increased potential for harm as a result of the growing capacity to collect, store and disseminate personal information. In the contemporary environment, a record is generated in a computer system or data bank each time a person makes a telephone call, utilizes an Internet-based service, uses a credit card or visits a health clinic. The potential for the cross-referencing and cross-matching of data sets from such different sources makes it possible to paint a very detailed picture of a person's lifestyle, religious and political views, health and shopping habits thus increasing the risk of fraud, unauthorized access and/ or targeting of individuals by parties, whether they be benign or malicious. It is the role of the policy maker to provide for the protection of the populace from such negative impacts, while encouraging the positives of commerce and efficiency.

---

2 For e.g. Universal Declaration on Human Rights 1948

3 www.cdt.org/privacy/guide/basic

This role is further complicated by the impact of the events in of September 11th, 2001, in the United States and subsequent terrorist attacks in other Countries such as Spain and England on national security concerns and the identification that access to information deemed personal may be critical to the identification of such activities by law enforcement authorities. The question which arises is how to balance improved demands for national security against the right to privacy, a challenge further elaborated upon in the discussion of lawful Interception of Communications.

The business environment is such that it is normal to use increasingly sophisticated electronic means to collect, store, transmit, process, and use personal data while the liberalization of trade in goods and services is making the collection, storage access, transmission, processing, and use of personal data more transnational in nature than ever. In order for e-commerce to continue to flourish it is essential that the protection of privacy is provided for without restricting the flow of information necessary to make e-commerce a powerful tool for both consumers and businesses.

This Report will review and analyse the contemporary frameworks for Privacy law as recommended by international organizations and implemented in other jurisdictions and trade blocks. The status of Privacy laws enacted by the beneficiary countries of the HIPCAR[4] ICT Legislative Framework Project will also be reviewed and assessed in the context of alignment to best international practice. These will together guide to the development of Policy Building Blocks which will be used as the foundation of a harmonized regional perspective on the issues associated with Privacy laws.

1.2 Executive Summary

This Assessment Report has been prepared in accordance with Phase 1 of the Work Plan for the Working Group on ICT Legislative Framework – Information Society Issues under the HIPCAR Project, which makes provision for a critical assessment report of E-Evidence existing in a number of States (the "Beneficiary Member States"[5]) in the Caribbean Region. This Assessment Report is for discussion and adoption by the HIPCAR Working Group on ICT Legislative Framework Meeting to be held in Saint Lucia on March 8th – 13th, 2010.

The purpose of this Assessment Report is to provide an analysis of the key issues and common principles reflected in ICT regulatory and legislative frameworks relating to the protection of privacy and personal information in the Beneficiary Member States and to provide a reference document for policy makers, legislators and regulators in the Beneficiary Member States that will serve as a basis for harmonized policy guidelines to be developed in Phase II of the Work Plan, and that may be used to produce model legislation under Phase III of the Work Plan.

Section 2.1 identifies the international and regional trends and best practices, which provide the basis for comparison with national laws, and eventual gap analysis.

Section 2.2 presents a comparative law analysis of a variety of international, regional, and national frameworks which address this particular issue. This review summarizes the intent and approach used in the framework, and also provides some insight into the administrative structure supporting the implementation of the legal framework

[4] The full title of the HIPCAR Project is: "Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures". HIPCAR is part of a global ITU-EC-ACP project carried out with funding from the European Union set at EUR 8 million and a complement of USD 500,000 by the International Telecommunication Union (ITU). It is implemented by the ITU in collaboration with the Caribbean Telecommunications union (CTU) and with the involvement of other organizations in the region. (See www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html).

[5] Antigua and Barbuda, The Bahamas, Barbados, Jamaica, the Commonwealth of Dominica, the Dominican Republic, Haiti, Grenada, Guyana, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Suriname and Trinidad and Tobago.

Section 2.3 identifies key trends and practices in the implementation of Privacy and Data Protection legal frameworks. This section provides a discussion of the key policy considerations associated with these trends, to provide a conceptual frame of what will be considered in the assessment of existing legislation.

Section 3.1 provides an overview of the current legislative environments in the Beneficiary Member States vis-à-vis the main issues associated with an effective legal framework for Privacy and Data Protection.

Section 3.2 undertakes an assessment of these legislative frameworks, comparing them against the key principles and trends identified in Section 2.3. This facilitates the critique and rating of key clauses within the legislative framework.

Section 3.3 provides a tabular summary of the comparisons undertaken in Section 3.2, providing a snap shot of the comparative state of current stage of legislative efforts in the Beneficiary Member Stages.

Thereafter in included the bibliography of materials researched as well as the sources of information considered in this Report.

Section II:
Overview on Work Done Internationally, Legislation and Key Elements

2.1 Work of International Organizations Relating to the Protection of Privacy

Several models of protection of privacy have evolved ranging from voluntary industry codes of practice and standards, to legislation and international conventions and guidelines. Among them are the Organisation for Economic Co-operation and Development (OECD), United Nations (UN), European Union (EU), and the Asia-Pacific Economic Co-operation (APEC).

2.1.1 Organisation for Economic Co-operation and Development

In 1980, the Organisation for Economic Co-operation and Development (OECD) adopted the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. These Guidelines have been identified by some as the oldest and perhaps most successful framework in force today, and accordingly, essentially all privacy laws in the world today seem to have been derived from the OECD's work. What is further notable about this policy framework is its apparent resistance to obsolescence by developments in information and communications technology sector. The Guidelines were developed to help harmonize national privacy legislation having regard to the danger that disparities in national legislations could hamper the free flow of personal data across frontiers which are ever increasing with the introduction of computer and communications technology. Restrictions on these flows would cause serious disruption and operational inefficiencies in important economic sectors, such as banking and insurance. The Guidelines represent international consensus on basic principles of what constitutes honest and trustworthy treatment of personal information and which can be built in to, or form the basis of, national legislation while recognizing human rights principles and the differences in legal and regulatory regimes of various countries.

The OECD Guidelines and the 1998 OECD Ottawa Declaration on Privacy are valuable in helping countries with different traditions develop effective privacy protection and avoid potential trade disputes based on data privacy concerns. In 2007 the OECD adopted the Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy that aims in particular at improving the domestic frameworks for privacy law enforcement to better enable the domestic authorities to co-operate with foreign authorities and at developing effective international mechanisms to facilitate cross-border privacy law enforcement.

2.1.2 United Nations

The United Nations (UN) General Assembly adopted the *Guidelines Concerning Computerized Personal Data Files* in December 1990. The *Guidelines* contain general principles concerning the minimum guarantees that should be provided in any national legislation dealing with the collection, storage, use and transmission of computerized data files. They include such principles as accuracy, specification and content, non-discrimination, security, and the free transborder flow of data in the presence of comparable safeguards.

Further, the human right to privacy protects the individual's private life against arbitrary, unlawful, or abusive interference. The Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), the American Convention on Human Rights (ACHR), and the European Convention on Human Rights (ECHR) each contains provisions protecting the right to privacy. The UN

Human Rights Committee, which interprets the ICCPR, has recognized core data protection principles as applicable to both public and private actors: generally,

> "[t]he gathering and holding of personal information on computers, databanks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law."

Accordingly, States that formulate data protection laws often perceive these laws as a necessary implementation of the right to privacy

2.1.3 European Union

Privacy in the processing of personal data and the confidentiality of communications are recognized as fundamental rights requiring protection in the European Union's Data Protection Directive 1995[6] and Privacy Directives[7] which are regarded the most detailed and complete set of regional privacy laws available in the world. The Directives concentrate on the European Common Market issues and have helped to a great extent to harmonize pan-European regulatory and implementation issues.

The Privacy Directive requires member States to harmonize and ensure an equivalent level of protection of the right to privacy with respect to personal data in the electronic communication sector. Pursuant to this, the Data Protection Directive prohibits the transfer of personal information to any country that does not have adequate privacy laws. As a result, European Union (EU) Member States have implemented legislation that prohibits the transfer of personal information from the EU to third countries unless such countries have adequate privacy protection in their laws.

2.1.4 Asia-Pacific Economic Cooperation

The work on a Privacy Framework being continued by Asia-Pacific Economic Cooperation (APEC) is deemed the most exciting initiative underway in the world with regard to providing international standards on privacy and personal data protection. APEC has built on the OECD Guidelines and has added the concepts of harm and accountability while re-affirming the value of privacy to e-commerce and to individuals. The principles-based APEC Privacy Framework is an important tool aimed at promoting e-commerce throughout the Asia-Pacific region by encouraging the development and implementation of appropriate protection of privacy of and ensuring free flow of information in the Asia Pacific region.

The APEC Privacy Framework also addresses issues which are particularly relevant to the economies of APEC Member States. Within this context it provides a balance between the protection of privacy of information and commercial interests while duly recognizing cultural and other diversities existing within the Member States.

The APEC Privacy Framework was developed in recognition of the importance of:

- Developing appropriate privacy protections for personal information, particularly from the harmful consequences of unwanted intrusions and the misuse of personal information;
- Recognizing the free flow of information as being essential for both developed and developing market economies to sustain economic and social growth;
- Enabling global organizations that collect, access, use or process data in APEC member economies to develop and implement uniform approaches within their organizations for global access to and use of personal information;

---

6 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (EU Data Protection Directive).

7 Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications).

- Enabling enforcement agencies to fulfill their mandate to protect information privacy; and,
- Advancing international mechanisms to promote and enforce information privacy and to maintain the continuity of information flows among APEC economies and with their trading partners[8].

2.2 Privacy Legislation Internationally

Introduction

Some States have developed and adopted legislation in an attempt to deal with privacy issues and find the ultimate balance between protecting the privacy needs of consumers and ensuring that information flows are not restricted in such a way as to inhibit the growth of electronic commerce. In some States while substantial legislation has been enacted relating specifically to privacy and data protection, in many cases the protection of personal information is not found in a single enactment but rather, in various enactments dependent on the type of personal information involved.

2.2.1 United Kingdom

The United Kingdom Data Protection Act 1998 implements data protection rules consistent with the provisions found in Directive 95/46/EC. The purpose of the Act is to protect the individual rights and freedoms of persons, in particular their right to privacy with respect to the processing of personal data. Failure to comply makes a person personally liable and such a person may incur a large fine and receive a criminal record. The Act applies to personal data (information about a natural person) whether it is held on a computer system or a piece of paper and the rules are more stringent with regard to certain sensitive data. The Act provides that personal data must be processed in accordance with certain principles and conditions. These conditions include the following: personal data can only be processed if:

(i) the individual has given consent;

(ii) it is part of a contract;

(iii) it is a legal obligation;

(iv) it is necessary to protect the individual; and

(v) it is in the legitimate interests of the data controller.

Consumer organizations consider that the Act is weak because the Data Protection Commission can only request compliance except where there is evidence of fraud and action may depend on the victims taking redress through the courts. General oversight of the implementation of the act is provided by the Information Commissioner's Office which is an independent office reporting to the Parliament, with the Ministry of Justice as its sponsor. It is an organization of about 200 persons that provides administrative oversight over a range of different legislative instruments. This represents considerable development from its first incarnation established in 1984 of 10 persons, primarily registering Data Controllers. The ICO has power to:

(i) conduct assessments to check that organizations are complying with the Act;

(ii) serve information notices requiring organizations to provide the ICO with specified information within a certain time period;

(iii) serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organizations to take (or refrain from taking) specified steps in order to ensure they comply with the law;

(iv) prosecute those who commit criminal offences under the Act;

[8] Ww2.austrlii.edu.au

(v) conduct audits to assess whether organizations' processing of personal data follows good practice; and

(vi) report to Parliament on data protection issues of concern.

2.2.2 Malta

The right to privacy is a fundamental human right, which is safeguarded and enshrined in the Constitution of Malta[9]. The enforcement of the right to privacy is facilitated by the protection of personal data from abuse. The Data Protection Act, Cap. 440 of Malta was the first law in Malta that directs itself exclusively to the protection of personal data. It was introduced in order to render Maltese law compatible with Directive 95/46/EC, even though at the moment of its introduction Malta was not a member state. This was partly to facilitate the transfer of data with EU member states, and partly in preparation for the potential accession of Malta to the EU.

The Data Protection Act, Cap. 440 makes provision for the protection of individuals against the violation of their privacy. It outlines nine principles of 'good information handling' to guarantee the protection of personal information which includes that:

- personal data is processed fairly and lawfully;
- personal data is only collected for specific, explicitly stated and legitimate purposes;
- personal data is not processed for any purpose that is incompatible with that for which the information is collected;
- personal data that is processed is adequate and relevant in relation to the purposes of the processing;
- personal data that is processed is correct and, if necessary, up to date;
- all reasonable measures are taken to complete, correct, block or erase data to the extent that such data is incomplete or incorrect, having regard to the purposes for which they are processed;

By virtue of the Data Protection Act, Cap. 440. Data collectors, such as educational institutions, employers and banks, are obliged to inform individuals of the reasons for collecting information about them. Furthermore, individuals are to be assured that the data collected will not be used for any other reason than that specified by the data collector. The act also contains accuracy requirements and specifies that 'explicit' consent from individuals is necessary in order to process 'sensitive personal data'.[10] Oversight of the Act is provided by the Data Protection Commissioner, an independent officer which reports to the Parliament through the Minister of Infrastructure, Transport and Communications.

2.2.3 Canada

In Canada, the Personal Information Protection and Electronic Documents Act came into force in January 2001. The Act establishes the rules for the protection and management of personal information that is collected, used or disclosed by private organizations during the course of commercial activities.

The fundamental tenets of the Act are:

(i) organizations that collect, use or disclose personal information during the course of commercial activity must do so only with the prior knowledge and consent of the affected individuals; and

(ii) such information may only be used for the purposes for which consent has been given.

[9] Constitution of Malta Act, 1964.

[10] See Malta Data Protection Act- found at www.sfa2005.eu/sites/default/files/Malta%20Data%20Protection%20Act.pdf

The Act limits the collection, use and disclosure of personal information to purposes that a "reasonable person" would consider appropriate in the circumstances. It will apply to any private enterprise that collects, uses or discloses personal information and will not be limited to businesses engaging in e-commerce or the electronic collection of data. Thus, information collected in a ballot box located in a supermarket will enjoy the same protection as personal data collected through online surveys. Oversight of the Act is facilitated through the establishment of the Office of the Data Commissioner. This is an officer of the Parliament, comparable to that of an Ombudsman. This is notable due to its inherent advocacy nature in its role as a watchdog.

The Act is based on the fair information principles set out in the Canadian Standards Association's Model Privacy Code for the Protection of Personal Information (the "CSA Code"). The CSA Code is the product of a collaborative effort between businesses, governments, academics, consumer associations and other privacy stakeholders. The principles of the CSA Code are incorporated (with some modifications) into the Act as Schedule 1 and private sector organizations must adhere to them.

2.2.4 United States of America

The United States of America (USA) does not have comprehensive privacy legislation at the federal level. It has enacted and relies on a mix of a series of industry or data-specific privacy laws, regulation, market forces and private sector codes of conduct to achieve protection of privacy:

These include:

1) the Children's Online Privacy Protection Act, which provides children under the age of 13 with special privacy protections; and
2) the Fair Credit Report Act which provides for the protection of data relating to credit reports; and
3) the USA Patriot Act[11] provides for the protection of personal information relating to citizenship and immigration.

2.2.5 Australia

Efforts to harmonize privacy provisions locally have been undertaken in Australia. A review of the Privacy Act was undertaken in Australia in 2005 and it was recommended by the Australian Privacy Commissioner that the Telecommunications Act and the Privacy Act be amended to provide consistency and to clarify what constitutes authorized uses and disclosures under each Act, and to ensure that the Privacy Act cannot be used to lower the standard of privacy protection provided by the Telecommunications Act.

The Federal Office of the Privacy Commissioner (PCO), Australia operates under the federal *Privacy Act 1988* and is an independent Office responsible for the protection of:

1) Personal information about an individual that is handled by Australian and ACT government agencies;
2) Personal information about an individual held by all large private sector organisations, all private sector health service providers and some small businesses;
3) Credit worthiness information held by credit reporting agencies and credit providers; and
4) Personal tax file numbers used by individuals and organisations.

2.2.6 EU – United States Safe Harbour Agreement

In addition to the industry or data-specific privacy laws referred to above, the United States and the European Union have entered into a safe harbour agreement that is designed to ensure the free flow of

[11] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act

personal data between the two parties. Without such an agreement, there were fears that the EU might begin to block data transfers to the United States on the grounds that it did not meet the Data Protection Directive's adequacy standard.

Although the Safe Harbour Agreement has been in place since 2000 and was thought to provide an effective solution bridging the United States – European privacy divide, United States support for the agreement has been tepid, at best. President George W. Bush has publicly questioned the agreement, noting his concern with the perception that the European Union is dictating United States privacy policy. With the notable exceptions of Microsoft and Intel, United States corporations have thus far been slow in signing up for the Safe Harbour Agreement.[12]

2.2.7 New Zealand

In New Zealand the protection of data is provided for in a number of laws including the Privacy Act 1993. New Zealand's Privacy Act of 1993 came into force on July 1, 1993, and has been amended several times. It regulates the collection, use and dissemination of personal information in both the public and private sectors. It also grants to individuals the right to have access to personal information about them held by any agency. The Privacy Act applies to "personal information," which is any information about an identifiable individual, whether automatically or manually processed. Recent case law has held that the definition also applies to mentally processed information. The news media are exempt from the Privacy Act in relation to their news activities.

The Act creates 12 Information Privacy Principles generally based on the 1980 Organization for Economic and Cooperation Development (OECD) Guidelines and the information privacy principles in Australia's Privacy Act 1988. In addition, the legislation includes a new principle that deals with the assignment and use of unique identifiers. The Information Privacy Principles can be individually or collectively replaced by enforceable codes of practice for particular sectors or classes of information. At present, there are three complete sector-specific codes of practice in force: the Health Information Privacy Code 1994, the Telecommunications Information Privacy Code 2003, and the Credit Reporting Privacy Code 2004 (which came into full effect on April 1, 2006). There are several codes of practice that alter the application of single information privacy principles: the Superannuation Schemes Unique Identifier Code 1995, the Justice Sector Unique Identifier Code 1998, and the Post-Compulsory Education Unique Identifier Code 2001. In addition to the information privacy principles, the legislation contains principles relating to information held on public registers; it sets out guidelines and procedures in respect to information matching programs run by government agencies, and it makes special provisions for the sharing of law enforcement information among specialized agencies. [13]

Oversight of the framework is provided by the Privacy Commissioner's Office, which is an independent office that reports to the Parliament through the Minister of Justice

[12] See Annex 4 Contribution by Professor Michael Geist University of Ottawa, Faculty of Law, Director of E-commerce Law, Goodmans LLP, found on www.itu.int/ITU-T/special-projects/ip-policy/final/Attach04.doc

[13] See www.privacyinternational.org/article.shtml?cmd[347]=x-347-559512

Section II

2.3 Key Elements of Privacy and Data Protection Frameworks

Introduction

There are a number of common principles that are outlined by the major data protection frameworks in force worldwide. These principles, from sources as varied as the OECD, UN and EU, can be summarized as:

- *Collection Limitation Principle* which states that there should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- *Data Quality Principle* which states that personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
- *Purpose Specification Principle which delineates that th*e purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
- *Use Limitation Principle* which seeks to ensure that personal data is disclosed, made available or otherwise used for purposes other than those specified in accordance with the purpose specification principle except either with the consent of the data subject; or the authority of law.
- *Security Safeguards Principle* which provides that personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
- *Openness Principle* which states that there should be a general policy of openness about developments, practices and policies with respect to personal data. Systems should be readily available to establish the existence and nature of personal data within an organisation, and the main purposes of their use, as well as the identity and usual residence of the data controller.
- *Individual Participation Principle* which gives an individual should have the right to obtain from a data controller, or otherwise confirmation of whether or not the data controller has data relating to him, be given reasons if a request made is denied, and to be able to challenge such denial; and to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
- *Accountability Principle* which states that a data controller should be accountable for complying with measures which give effect to the principles stated above.
- *Non-discrimination Principle* which states that sensitive information should not be processed, unless particular, identified conditions are met.
- *Limitation of Transborder Data Flows* which states that personal information should not be transferred from one jurisdiction to another without equal or greater protections to privacy and information protection.; and
- *Supervision and Sanctions* which encourages the law of every country to designate an authority which, in accordance with its domestic legal system, is to be responsible for supervising observance of the principles set forth in the framework.
- *Power to Make Exceptions* recognizes the need, from time to time for departures from the principles referenced above may be authorized only if they are necessary to protect national security, public order, public health or morality, as well as, the rights and freedoms of others, especially persons being persecuted (humanitarian clause) provided that such departures should be expressly specified in law which expressly states their limits and sets forth appropriate safeguards.

The following section reviews the key considerations associated with the enactment o f these Principles.

2.3.1 Legal Mandate

Key questions to be addressed with respect to the legal mandate for privacy and data protection are:

- 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?

2.3.1.1 Of primary concern in the establishment of a framework that is geared to reinforce the basic tenet of privacy in law, is ensuring that there is appropriate legitimacy given to this new framework in conjunction with the systems and processes already established. The fundamental principles guiding the establishment of Privacy and Data Protection regimes is the determination of an appropriate balance of the benefit to the State of civil registries, and the right of the individual that such registries are not utilised without their approval.

2.3.1.2 It is in this context that OECD identified the *"Collection Limitation Principle"* which attempts to achieve that balance by providing the individual on whom data is collected the opportunity to be informed of the reason for the collection of that information, and be assured that the information will not be used for any other reason than that to which they have consented. In this way, some level of control is retained by the individual on how their information is to be used, and provides them with the opportunity to opt out of any proposed utilization of which they are wary. The implication for the implementation of this Principle is the notification, in at least writing, to the client of a service of the reason why the information is needed for the provision of the services or goods.

2.3.1.3 It is notable that initially the frameworks that eventually developed into contemporary privacy and data protection laws were initiated by the need to manage the way in which Governments and Public Authorities managed such information, especially with the onset of computerised processing systems which allowed the easy, seamless electronic dissemination of such information. It is in this initial context that much discourse on the administration of privacy and data protection regimes are framed. However, with the growing utilization of public-private partnerships where certain processing functions are outsourced to private enterprise, this conceptualization of the limits of oversight of the legislation needs to be reevaluated. Further consideration of the contemporary environment finds that the quantum and nature of information which can and is captured when the private sector engages the public can surpass that captured by the public sector. Also, cognizant of the private sector's deployment of similar information systems, the case has been readily made that the risks and threats to the general public, and the individual, associated with this information being mismanaged by the public sector may be surpassed with inappropriate management of that information by the private sector. In that regard, the United Nations' Guidelines of 2000 recognized in its "Applicability Principle" that frameworks of privacy protection should place obligations not only on the public sector, but the private sector as well.

2.3.1.4 The United Nations went further in this regard with the establishment of the "*Principle of Non-discrimination"* which identifies a subset of personal information which, due to their nature as being the historic basis of social discrimination and exclusion, are to be restricted from being collected in a mandatory fashion. This is not to say however that there is no such use for that information as, for example, in the development of demographics and statistics of a population. However, this principle

underscores that such should not be considered in the provision of service or the determination of award by public and private entities. The implication of this principle is that unless such is particularly necessary in the provision of the service or goods, those information fields requesting such information should at the least be non-essential or optional, and at the worst be excised from forms of application.

2.3.1.5 Despite the goals espoused on 2.3.1.2 above, it is recognized that there are particular sectors of activity, necessarily executed by the State and other, which require the autonomy to treat with information about individuals in a manner that by its nature, precludes consent of the individual. Particular matters in the realms of National Security and Public Health management have been noted to be categorized in this manner. Therefore while it is incumbent upon the legal system of each jurisdiction to establish frameworks to mitigate against abuse, a comprehensive regime of privacy protection will include provisions which provide the administration the "*Power to Make Exceptions"* as noted by the United Nations in the 1990 Resolution.

2.3.2 Institutional Framework

Key questions to be addressed with respect to institutional framework are:

- 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?

2.3.2.1 Once the legal mandate for a privacy protection regime is established and the basic tenets enshrined in statute it is necessary to establish an administrative framework through which the law will be enabled. Again, the United Nations explicitly noted that an oversight authority would needs to be established to bring the framework into effect.

2.3.2.2 The European Commission also noted the same in the 1995 Directive, stating that;

> *" A fully-fledged system of protection of personal data not only requires the establishment of rights for data subjects and obligations for those who process personal data, but also appropriate sanctions for offenders and monitoring by an independent supervisory body."*

Accordingly, a critical component of an effective privacy policy framework is the requirement for independent oversight to oversee to compliance by the data controller with privacy legislation and policy by, among other things:

- monitoring how the legislation is administered and conducting reviews;
- initiating privacy compliance investigations;
- resolving and mediating privacy complaints; and
- providing review and oversight impact assessments relating to privacy;

2.3.2.3 Given that this functionary will be required to investigate and audit Public Authorities, and investigate the actions of senior public officials, the institutional framework to provide this privacy oversight should be free from the influence of political or commercial influence, and in the course of his duties should take instructions from no person or office. Accordingly, the frameworks should explicitly

provide appointment (and removal) of an independent officer – a Data Protection Commissioner, with a maximum term of office for set for a period which is longer that the election cycle of the Political Executive. Notwithstanding this factor, there is the consideration that the Data Protection Commissioner provides a form of regulatory oversight of persons in the private sector. This is traditionally a role of the Political Executive. Accordingly, in determining the appropriate locus of the oversight body, appropriate balance must be maintained between these competing paradigms. A review of contemporary establishment finds the incumbent should have general experience and knowledge in the fields of privacy protection, and have no other occupation save for this function. From a perspective of continuity, the appointment of the Data Protection Commissioner has been found to be accompanied by the appointment of a Deputy Data Protection Commissioner, whose qualifications are similar to that of the Commissioner, and who shall act as the Commissioner on the absence of the incumbent.

2.3.2.4 As another aspect of this independence, the Commissioner should be charged with distinct legal personality so that the Commissioner is capable of entering into contracts, acquiring, holding and disposing of any kind of property for the purposes of his or her functions, suing and being sued, and doing all such things and entering into all such transactions as are incidental or conducive to the exercise or performance of his functions under the Act.

2.3.2.5 Further, in order to preserve the independence and impartiality of the Commissioner, consideration should be given to the protection of the Commissioner from liability in respect of an act done or omitted to be done in good faith in the exercise or purported exercise of his or her functions. That protection should not extend in cases of personal injury. Additionally, provision should be made in the legal framework to indemnify the Commissioner for the cost of defending actions.

2.3.2.6 From a matter of practicality, the Commissioner will not work alone, and will lead an agency. This agency will be staffed by personnel in accordance with an organisational structure defined by the Commissioner. To support the investigative and audit operations of the office, the Commissioner should be empowered to delegate any of his or her investigative and enforcement powers conferred upon him by the law to any authorized officer designated for that purpose.

As confidentiality is a key aspect to a privacy protection framework, the Commissioner, Deputy Commissioner and other relevant members of staff should be required to take the oath not to divulge any data obtained as a result of the exercise of a power or in the performance of a duty under the Act except in accordance with this Act or any other enactment or as authorized by the order of a Court.

2.3.3 Regulatory Empowerment

Key questions to be addressed with respect to the Regulatory Empowerment of the framework are:

- 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?

2.3.3.1 In accordance with guidance from the European Commission which espouses that it is essential that the Data Protection framework is supported by an appropriate enforcement regime, the Commissioner should be empowered as a regulator for the purpose of carrying out his functions; to do all such acts as appear required, advantageous or convenient for the carrying out of these functions. These powers may include the power to undertake audits, investigate complaints, and to obtain information about documentation, processing and security of data. The Commissioner should be empowered to request that a person to furnish to him access to personal data stored. These powers should be linked to

an enforcement regime. Such an enforcement regime should include provisions where failure to comply with a request of, or notice by, the Commissioner for information is to be treated as an offence.

2.3.3.2 As a consequence of the imposition of such a regulatory framework, it has to be assumed that any organisation that manages personal information is therefore responsible for the appropriate management of that information in accordance with the privacy guidelines proposed by this framework. As early as the 1980 OECD Guidelines the *Accountability Principle's* imposition of such responsibility has been recommended in such frameworks. This accountability, along with an enforcement regime that is systematically engaged, provides the regulatory pressure that will encourage the change in attitude and practice that will meaningfully adjust attitudes to the treatment of personal information.

2.3.3.3 In the spirit of good regulatory practice and administration, the regulatory regime should include the definition of key practices, metrics and guidelines which will facilitate the ready review of privacy protection practices of an organization. The OECD recognized this with the *Openness Principle*

2.3.4 Considerations for Collection of Personal Information

Key questions to be addressed with respect to the consideration for the collection of personal information in the framework are:

- 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

2.3.4.1 Unlike the question of administrative governance, when there is consideration of issues surrounding the collection of personal information, the guidance from best practice is extremely consistent. The third identified OECD principle of *Purpose Specification,* where the data subject is notified of the reason for the collection of data is fundamental to the empowerment of the individual. First, this principle elaborates on the prior requirement for consent, as this principle assures that the individual consents when in a position of knowledge. So critical is this principle that it is emulated in United Nation's 1990 Guidelines and the European Union Directive of 1995. Secondly, this principle supports the requirement for consent by limiting the subsequent use of the information to that which the individual was informed.

2.3.4.2 With that specification of purpose, there is the limitation of what information is needed for that purpose. The individual therefore has the right to refuse to submit information which is not relevant for the stated purpose without penalty or disadvantage in the provision of the service or good. Again, these principles are empowering the individual in their interaction with the party capturing this information.

2.3.4.3 Notwithstanding the importance of the individual's control of how their personal information is used, in the particular instances of Health Care Management and National Security, adherence to such principles is unworkable. In the case of health care management, where either the individual is probably ignorant of the intricacies of health care sciences or where the medical professional is undertaking investigations before the determination of a diagnosis, the adherence to these principles, and the restrictions on the processing of sensitive personal information would make health care impossible. Similarly, in the sphere of national security, it is impractical for the security services to inform a subject of surveillance of same. Therefore in these particular cases specific legislative frameworks have been

developed to properly address practical questions of processing the information while providing the necessary protection to the individual's privacy.

2.3.5 Considerations for the Storage and Use of Collected Information

Key questions to be addressed with respect to the consideration for the storage and use of information collected in the framework are:

- 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

2.3.5.1 Building on the power of assent given to the data subject at the point of information collection, the individual's empowerment of how information collected is processed after capture is also a critical aspect of contemporary data protection and privacy frameworks. Developing on the concept the information captured must only be relevant for the stated purpose, and should only be used for the stated purpose, it stands to reason that the individual should be informed of any other purpose that the information is to be used for as enrollment to each processing phase warrants the assent of the data subject/ individual. Referred to the *Use Limitation* Principle, this obligation of the framework is geared to engender confidence that a person's information is not being "mined" without their knowledge. Further, the United Nation's Guidelines adds the additional concept that the collector of information should not retain the personal information for a period longer than that is required for the purpose specified. This relevant period of retention will necessarily include any other legal or regulatory requirements in force for that operation with regard to the retention of records.

2.3.5.2 The OECD model framework also posited that it is essential that the information stored about an individual should be correct and accurate. This is essential so that the information when processed treats with the individual fairly and appropriately. That the collecting/ processing organization has this responsibility for assurance of this *Data Quality (Accuracy) Principle* is in line with overarching *Accountability Principle* discussed above. Notably, in this regard, the United Nations noted that the transborder nature that can be associated with the fusion of global telecommunications systems (like the Internet) and electronic information management systems:

> *It is desirable that the provisions of this principle should apply to everyone, irrespective of nationality or place of residence.*

2.3.5.3 In this regard, the individual on whom the data relates is considered the best person to verify the information stored. Accordingly, while the OECD's *Data Quality (Accuracy) Principle* proposes an obligation on the party storing the information to ensure that it is "relevant", "accurate, complete and up-to-date", the *Individual Participation Principle* gives the individual, once their identity is proven, the right to request from the organization the information kept about them. If on review of the information the individual seeks to challenge the validity of particular aspects of the information stored, the individual may cause the organization to correct the information in its store. This right however is not unfettered. It is recognized that this provision of access may leas to the divulgence of personal information of other persons to the requesting individual. Therefore the organization is responsible for ensuring the individual's identity, requesting evidence of any modification demanded, and redacting all sensitive information not associated with the requesting individual in the release of the information. Further,

recognizing that a deluge of requests can lead to the disruption of the organization's function, there are a number of frameworks which provide for organization to deny the provision of access in particular circumstances, such as where the information is otherwise readily available, where the request is deemed vexatious and purposefully disruptive.

2.3.5.4 Confidentiality and security are key aspects of the protection of privacy. As such, the organization that is processing personal information must ensure that sufficient security systems are in place to protect the information from unauthorized access or intrusion, destruction or other forms of compromise. Again the responsibility of the organization controlling the information, the *Security Principle* mandates the use of appropriate filing, categorization and management of records, in either physical (paper or cards) or electronic form.

2.3.6 Considerations for the Disclosure of Collected Information

Key questions to be addressed with respect to the consideration for the disclosure of information collected in the framework are:

- 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?

2.3.6.1 Management of disclosure is as critical to the privacy protection regime as the collection and storage of the personal information of data subjects. In accordance with the general philosophy of allowing the individual to have some level of transparency to their information under the control of an organization, international best practice encourages the notification to the consumer of any intention to disclose information to third parties. Such notification can be facilitated at the time of information capture, or at some time thereafter, once it is before the disclosure is effected.

2.3.6.2 Notwithstanding this general philosophy, as with 2.3.4.3 above, there are particular circumstances where such notification before disclosure is not practical (as in Health Care facilitation) or practical (as in the case of law enforcement or due to a request of a judicial Order). This has been recognized and elaboration upon in the frameworks developed by the OECD, UN and EU. Accordingly, the framework should include an outline of exemptions for when disclosure will be facilitated in the absence of the data subject.

2.3.6.3 While the OECD framework did not elaborate on the principle of *Transborder Data Flows,* the United Nations' Guidelines of 1990 and the European Union 1995 Directive reinforce the need to ensure that the privacy protections established by the home jurisdictions are at least matched in the jurisdiction to which the data is being transferred. In the interest of facilitating some level commerce, these frameworks do provide, however, for the limited transfer of information in such that commerce across borders can be facilitated to that extent to which the Security obligation of the organization controlling the information is maintained. Accordingly it is imperative that new frameworks developed geared to interact in the aspects of trade in which personal information is critical must include such provisions to control transborder data flows.

Section III:
Analysis of Regional Texts and Presentation of International Best Practices

3.1 Status of Privacy Legislation in Beneficiary States

Introduction

Only one beneficiary Member State is reported to have substantial privacy legislation in force on their statute books, namely the Bahamas. While Barbados has some aspects of privacy protection in statute, the framework thereby facilitated is not comprehensive. In the case of Saint Vincent and the Grenadines, Privacy Act, No.18 of 2003, which is a creditable framework, has been on the statute book since 2003 it has no legal force, as no date has been fixed for its commencement. St Lucia and Trinidad and Tobago also have proposed Bills laid before their respective Houses which were evaluated for conformance. Generally, these were found to be consistent with international best practice.

3.1.1 The Bahamas

The Bahamas Government introduced a series of Acts in 2003 including the Data Protection (Privacy of Information) Act designed to facilitate the development of e-commerce and e-government in The Bahamas. The Data Protection (Privacy of Information) ensures internationally recognized standards for the collection, use and disclosure of personal information by providing a statutory framework for the universal standards for data protection as found in the OECD Principles on Privacy 1980. A Data Protection Commissioner was appointed for The Bahamas with responsibility for the administration and enforcement of the provisions of the Act. Duties of the Data Commissioner include investigation of any contraventions of the legislation, and to provide information to the public about the legislation.

3.1.2 Saint Vincent and the Grenadines

The Privacy Act enacted in Saint Vincent and Grenadines regulates the collection, use, maintenance, disclosure and disposition of personal information by public authorities and provides rights to certain individuals about whom personal information is maintained. The regulatory approach adopted in the Privacy Act is principles-based, which was the approach adopted in 1980 by the OECD in the development of its eight guidelines on the Protection of Privacy.

It is notable that the Act does not apply to the private sector, and affords no protection for personal data that may be in that domain. There is also no provision in the Act which provides for the request of access to personal information. This may have been omitted as a person can acquire such access from a public authority under the Freedom of Information Act. As a result of the foregoing, the provisions of the Freedom of Information Regulations which deal with request for access to official documents will apply by virtue of section 15 of the Privacy Act which speaks to access being given to personal information under any of the enactment.

3.1.3 Frameworks in Development and Associated Trends

Across the region there are two proposed Bills that were laid in the Parliaments of the respective jurisdictions but not yet passed, in St. Lucia and Trinidad and Tobago. These frameworks, like that of Bahamas cleave fairly closely to the Eight Privacy Principles identified by the OECD's 1980 Benchmark framework. While the Bahamas legislation is principle-based and not prescriptive in nature, comparatively both of these new frameworks elaborate significantly on the base principles; with the Trinidad and Tobago the most elaborate of them all.

On consideration of particular points of policy where the frameworks under review diverged, it is notable that the St. Lucia legislative framework requires the registration of data controllers, a regulatory obligation not mirrored in any of the regional frameworks.

Also notable is that St. Vincent and the Grenadines and Trinidad and Tobago both do not envisage the establishment of a Commissioner appointed by the sole discretion of the Head of State. However, while Trinidad and Tobago proposed a dedicated Commissioner, St Vincent's is the only legal framework does not envision such. St Vincent is also the only framework where the obligation of information and privacy protection is limited to the private sector. These seem to be the most significant forms of policy divergence identified.

3.2 Assessment of Regional Texts

This Section presents a snapshot of how the key issues listed above are reflected in legal and regulatory texts from the beneficiary countries under the HIPCAR Project (Antigua and Barbuda, The Bahamas, Barbados, Belize, Dominica, Dominican Republic, Grenada, Guyana, Haiti, Jamaica, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Suriname, and Trinidad and Tobago), thereby classifying the situation in the beneficiary countries as related to administration of Privacy and Data Protection in categories ranging from poor (texts do not make reference at all to key issues) to fair (there is some mention of the issue but it is not detailed or not at an appropriate level, e.g. in some form of consultation document or draft regulation or even in a regulation which is not in line with primary legislation) to good (the texts reflect all elements categorized under a key issue).

Overview of Assessment Ratings:

GOOD: Provisions in law exist which address all major concepts identified by best practice

FAIR: Provisions in law exist which address some of the concepts identified by best practice

POOR: Provisions in law exist which do not adequately address concepts identified in best practice

NONE: There are no provisions in the law which address concepts identified.

LIMITED: There is no law in force which address the issue, however there are such provisions identified in legislation which may have not completed the law-making process (e.g. in legislation laid in the legislature but not passed at the time of report compilation)

* Bills laid before Parliament, not yet passed as statute

Section III

3.2.1 Legal Mandate

International Best Practices and Regional Trends:

- There is a clear legal mandate protecting privacy and personal information
- The framework is applicable to both the public and private sectors
- The framework clearly outlines the condition that personal information should only be collected with the consent of the subject of that personal information
- The framework limits the processing of 'sensitive information'
- The framework outlines conditions of exemption from the guidelines therein

Regional Examples

Antigua and Barbuda – NONE

Bahamas – GOOD – Clear delineation that the scope of oversight covers both public and private sectors. Clear definition of sensitive personal information as a matter of particular consideration.

"data controller" means a person who, either alone or with others, determines the purposes for which and the manner in which any personal data are, or are to be, processed;

"personal data" means data relating to a living individual who can be identified either from the data or from the data in conjunction with other information in the possession of the data controller

"sensitive personal data" means personal data relating to –

(a) racial origin;
(b) political opinions or religious or other beliefs;
(c) physical or mental health (other than any such data reasonably kept by them in relation to the physical or mental health of their employees in the ordinary course of personnel administration and not used or disclosed for any other purpose);
(d) trade union involvement or activities;
(e) sexual life; or
(f) criminal convictions, the commission or alleged commission of any offence, or any proceedings for any offence committed, the disposal of such proceedings or the sentence of any court in such proceedings.

3. (1) This Act binds the Crown.

(2) Where a government agency, satisfies the conditions for being a data controller or a data processor under this Act, the head of such institution shall be deemed, for the purposes of this Act, to be a data controller or, as the case may be, a data processor.

(3) For the purposes of this Act, as respects any personal data, all other public officers or employees, as the case may be, within the same institution, shall be deemed to be employees of the designated head in the case of a designation provided for in subsection (2).

4.(1) Except as otherwise provided for herein, this Act applies to a data controller in respect of any data only if -

(a) the data controller is established in The Bahamas and the data are processed in the context of that establishment; or
(b) the data controller is not established in The Bahamas but uses equipment in The Bahamas for processing the data otherwise than for the purpose of transit through The Bahamas.

Section III

(2) A data controller falling within subsection (1)(b) must nominate for the purposes of this Act a representative established in The Bahamas.

(3) For the purposes of subsections (1) and (2), each of the following is to be treated as established in The Bahamas –

(a) an individual who is ordinarily resident in The Bahamas;
(b) a body incorporated or registered under the laws of The Bahamas;
(c) a partnership or other unincorporated association formed under the laws of The Bahamas; and
(d) any person who does not fall within paragraph (a), (b) or (c) but, maintains in The Bahamas an office, branch or agency through which he carries on any business activity or a regular practice.

5. This Act shall not apply to personal data -

(a) that in the opinion of the Minister or the Minister for National Security are, Or at any time were, kept for the purpose of safeguarding the security of The Bahamas;
(b) consisting of information that the person keeping the data is required by law to make available to the public;
(c) kept by an individual and concerned only with the management of his personal, family or household affairs or kept by an individual only for recreational purposes;
(d) deliberations of Parliament and Parliamentary committees; or
(e) pending civil, criminal or international legal assistance procedures.

6.(1) A data controller shall comply with the following provisions in relation to personal data kept by him –

(a) the data or the information constituting the data shall have been collected by means which are both lawful and fair in the circumstances of the case;
(b) the data is accurate and, where necessary, kept up to date, (except in the case of back-up data);
(c) the data –
    (i) shall be kept only for one or more specified and lawful purposes,
    (ii) shall not be used or disclosed in any manner incompatible with that purpose or those purposes,
    (iii) shall be adequate, relevant and not excessive in relation to that purpose or those purposes, and
    (iv) shall not be kept for longer than is necessary for that purpose or those purposes, except in the case of personal data kept for historical, statistical or research purposes; and
(d) appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction.

(2) In determining for the purposes of subsection (1)(a) of this section, whether personal data or information constituting such data are fair in the circumstances of the case, regard is to be had to the method by which they are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be processed:

Provided however that the data or the information constituting such data shall not be regarded for the purposes of subsection (1)(a) of this section as having been obtained unfairly by reason only that its use for any such purpose was not' disclosed when it was obtained, if the data are not used in such a way that damage or distress is, or is likely to be, caused to any data subject.

Section III

(3) A data processor shall, as respects personal data processed by him, comply with subsection (1)(d) of this section.

7. Subsection (1)(a) of section 6 shall not apply to information intended for inclusion in data, or to data, kept for a purpose mentioned in paragraph (a) of section 9, in any case in which the application of that paragraph to the data would be likely to prejudice any of the matters mentioned in paragraph (a) of section 9.

Barbados – POOR – Applicability of provision limited to electronic signatures and does not consider other forms of personal information
[Electronic Transactions Act, CAP. 308B]

"data controller" means a person who, either alone, jointly or in common with other persons, determines the purposes for which and the manner in which any personal electronic signature service is, or is to be, processed

Belize – NONE

Dominican Republic – NONE

Dominica, Grenada – NONE

St. Kitts and Nevis – LIMITED – Draft legislation is reported to be in preparation before presentation to Parliament, and is as such confidential. Copies of the draft were not available for assessment.

St. Vincent and the Grenadines – FAIR – the Act neither identifies a "sensitive information distinctly, nor makes the provisions of the Act applicable to both private and public sectors. The Act is geared to managing the conduct of public authorities only. Further, there (are no provisions providing for necessary exemptions due to national security etc.)

"personal information" means information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing -

(a) information relating to the race, sex, national or ethnic origin, religion, age or marital status of the individual;
(b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved or which refers to the individual;
(c) any identifying number, symbol or other particular assigned to the individual;
(d) the address, fingerprints, 'Deoxyribo-Nucleic Acid' or blood type of the individual;
(e) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual;
(f) correspondence sent to a public authority by the individual that is explicitly or implicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence; or
(g) the views or opinions of any other person about the individual;

6. This Act shall bind the State.

St. Lucia* – LIMITED (GOOD) – Scope of application clearly includes both public and private sectors. Notable that "sensitive personal information" is NOT distinctly treated with.
[Privacy and Data Protection Bill, 2007]

"data controller" means a person who, either alone or with others process data or determines the purposes for which and the manner in which any personal data is or is to be processed;

Section III

"data subject" means the natural person who is the subject of personal data;

"personal data" means information about a data subject that is recorded in any form including, without restricting the generality of the foregoing-

(a) information relating to the race, national or ethnic origin, religion, age, sexual orientation, sexual life or marital status of the data subject;
(b) information relating to the education, medical, criminal or employment history of the data subject or information relating to the financial transactions in which the individual has been involved or which refers to the data subject;
(c) any identifying number, symbol or other particular designed to the data subject;
(d) the address, fingerprints Deoxyribo Nucleic Acid, or blood type of the data subject;
(e) the name of the data subject where it appears with other personal data relating to the data subject or where the disclosure of the name itself would reveal information about the data subject;
(f) correspondence sent to an establishment by the data subject that is explicitly or implicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence; or
(g) the views or opinions of any other person about the data subject;

3. (1) Except as otherwise provided in this Act applies to a data controller in respect of any data if-

(a) the data controller is established in Saint Lucia and the data is processed in the context of the business of that establishment; or
(b) the data controller is not established in Saint Lucia but uses equipment in Saint Lucia for processing data otherwise than for the purpose of transit through Saint Lucia.

(2) A data controller falling within subsection (1)(b) shall nominate for the purposes of this Act a representative established in Saint Lucia.

4. For the purposes of section 3 each of the following is to be treated as established in Saint Lucia-

(a) an individual who is ordinarily resident in Saint Lucia or the Caribbean Community;
(b) a body incorporated under the Companies Act, Cap. 13.01;
(c) a partnership or other unincorporated association formed under the laws of Saint Lucia; and
(d) any person who does not fall within paragraphs (a), (b) and (c) but maintains in Saint Lucia an office, branch or agency through which he carries on any activity related to data processing.

Crown to be bound
5. This Act binds the State.

Guyana – NONE

Jamaica – NONE

Trinidad and Tobago – LIMITED (GOOD) – despite a need to review the drafting to treat with apparent overlap in definitions provided for "*personal information*" and "*sensitive personal information*".
[Data Protection Bill, 2009]

"personal information" means information about an identifiable individual that is recorded in any form including–

(a) information relating to the race, nationality or ethnic origin, religion, age or marital status of the individual;

Section III

(b) information relating to the education or the medical, criminal or employment history of the individual or information relating to the financial transactions in which the individual has been involved or which refers to the individual;
(c) any identifying number, symbol or other particular designed to identify the individual;
(d) the address , fingerprint s, Deoxyribonucleic Acid or blood type of the individual;
(e) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual;
(f) correspondence sent to an establishment by the individual that is explicitly or implicitly of a private or confidential nature, and relies on such correspondence which would reveal the contents of the original correspondence; or
(g) the views and opinions of any other person about the individual;

"sensitive personal information" means personal information on a person's–
(a) racial or ethnic origins;
(b) political opinions;
(c) religious beliefs or other beliefs of a similar nature;
(d) physical or mental health or condition;
(e) sexual orientation or sexual life; or
(f) criminal or financial record;

3. This Act binds the State.

4. The object of this Act is to ensure that protection is afforded to an individual's right to privacy and the right to maintain sensitive personal information as private and personal.

5. This Act shall not–
(a) limit information available by law to a party in any proceeding;
(b) limit the power of a court or tribunal to compel a witness to testify or to compel the production of a document or other evidence; or
(c) apply to notes prepared by or for an individual presiding in a court of Trinidad and Tobago or in a tribunal if those notes are prepared for that individual's personal use in connection with the proceedings.

6. The following principles are the General Privacy Principles which are applicable to all persons who handle, store or process personal information belonging to another person:
(a) an organization shall be responsible for the personal information under its control;
(b) the purpose for which personal information is collected shall be identified by the organization before or at the time of collection;
(c) knowledge and consent of the individual are required for the collection, use or disclosure of personal information;
(d) collection of personal information shall be legally undertaken and be limited to what is necessary in accordance with the purpose identified by the organization;
(e) personal information shall only be retained for as long as is necessary for the purpose collected and shall not be disclosed for purposes other than the purpose of collection without the prior consent of the individual;
(f) personal information shall be accurate, complete and up-to-date as is necessary for the purpose of collection;
(g) personal information is to be protected by such appropriate safeguards necessary in accordance with the sensitivity of the information;
(h) sensitive personal information is protected from processing except where otherwise provided for by written law;

(i) organizations are to make available to individuals documents regarding their policies and practices related to the management of personal information except where otherwise provided by written law;

(j) organizations shall, except where otherwise provided by written law, disclose at the request of the individual, all documents relating to the existence, use and disclosure of personal information, such that the individual can challenge the accuracy and completeness of the information;

(k) the individual has the ability to challenge the organization's compliance with the above principles and receive timely and appropriate engagement from the organization; and

(l) personal information which is requested to be disclosed outside of Trinidad and Tobago shall be regulated and comparable safeguards to those under this Act shall exist in the jurisdiction receiving the personal information.

International Examples and Regional Harmonization

OECD

Collection Limitation Principle

OECD (1980) Principle 1 – There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

United Nations

Guidelines Concerning Computerized Personal Data Files (1990)

Lawfulness And Fairness

UN (1990) 1 – Information about persons should not be collected or processed in unfair or unlawful ways, nor should it be used for ends contrary to the purposes and principles of the Charter of the United Nations.

Power to Make Exceptions

UN (1990) 6 – Departures from [UN (1990)] principles 1 to 4 may be authorized only if they are necessary to protect national security, public order, public health or morality, as well as, inter alia, the rights and freedoms of others, especially persons being persecuted (humanitarian clause) provided that such departures are expressly specified in a law or equivalent regulation promulgated in accordance with the internal legal system which expressly states their limits and sets forth appropriate safeguards.

Exceptions to [UN (1990)] principle 5 relating to the prohibition of discrimination, in addition to being subject to the same safeguards as those prescribed for exceptions to principles I and 4, may be authorized only within the limits prescribed by the International Bill of Human Rights and the other relevant instruments in the field of protection of human rights and the prevention of discrimination.

Principle of Non-discrimination

UN (1990) 5 – Subject to cases of exceptions restrictively envisaged under [UN (1990)] principle 6, data likely to give rise to unlawful or arbitrary discrimination, including information on racial or ethnic origin, colour, sex life, political opinions, religious, philosophical and other beliefs as well as membership of an association or trade union, should not be compiled.

Section III

European Union
DIRECTIVE 95/46/EC

Article 3 – Scope

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Directive shall not apply to the processing of personal data:

- in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,
- by a natural person in the course of a purely personal or household activity.

Article 4 – National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
   (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;
   (b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;
   (c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

SPECIAL CATEGORIES OF PROCESSING

Article 8 – The processing of special categories of data

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

3.2.2 Institutional Framework

International Best Practices and Regional Trends:

- The framework makes it clear who is responsible for ensuring compliance to the obligations outlined.
- The oversight body shall be a distinct legal person, who takes direction from no other person in the execution of his duty.
- The oversight body is independent of the persons who would be responsible for the collection and use of personal information, including Government and private sector interests.
- This oversight body is afforded powers and privileges necessary to support its functions.
- This oversight body has recourse to channels of enforcement to ensure compliance.

Regional Examples

Antigua and Barbuda – NONE

Bahamas – GOOD – clear articulation of powers and responsibility of the oversight authority. With appointment at the sole discretion of the Head of State and strong entrenchment provisions, independence of decision-making is assured.

14.(1) For the purposes of this Act, there shall be a person who shall be known as the Data Protection Commissioner and who shall perform the functions conferred on him by this Act.

(2) The Commissioner shall be a corporation sole.

(3) The provisions of the Second Schedule shall have effect in relation to the Commissioner.

20. (1) The Commissioner may encourage trade associations and other bodies representing categories of data controllers to prepare codes of practice to be complied with by those categories in dealing with personal data.

(2) The Commissioner may approve of any code of practice so prepared (referred to subsequently in this section as a code) if he is of opinion that it provides for the data subjects concerned protection with regard to personal data relating to them that conforms with that provided for by sections 6, 8 (other than subsection (9)) and 10 and shall encourage its dissemination to the data controllers concerned.

(3) Any such code that is approved by the Commissioner shall be laid by the Minister before each House of Parliament and shall be subject to affirmative resolution of each House.

(4) In subsection (3), "affirmative resolution of each House" means that such code shall not come into operation unless and until affirmed by a resolution of each House of Parliament.

(5) This section shall apply in relation to data processors as it applies in relation to categories of data controllers with the modification that the references in this section to the said sections shall be construed as references to subsection (1)(d) of section 6 and with any other necessary modifications.

21.(1) The Commissioner shall in each year after the year in which the first Commissioner is appointed prepare a report in relation to his activities under this Act in the preceding year and cause copies of the report to be laid before each House of Parliament.

Section III

(2) Notwithstanding subsection (1), if, but for this subsection, the first report under that subsection would relate to a period of less than six months, the report shall relate to that period and to the year immediately following that period and shall be prepared as soon as may be after the end of that year.

SECOND SCHEDULE

1. The Commissioner shall be a corporation sole and shall be independent in the performance of his functions.

2. (1) The Commissioner shall be appointed in writing by the Governor-General acting on the advice of the Prime Minister after consultation with the Leader of the Opposition.

(2) The Commissioner -

(a) may at any time resign his office as Commissioner by letter addressed to the Governor-General and the resignation shall take effect on and from the date of receipt of the letter;

(b) may at any time be removed from office by the Governor-General on the advice of the Prime Minister after consultation with the Leader of the Opposition if, in the opinion of the Prime Minister, he has become incapable of effectively performing his functions or has committed a misbehaviour; and

(c) shall, in any case, vacate the office of Commissioner on reaching the age of sixty-five years.

3. The term of office of a person appointed to be the Commissioner shall be such term not exceeding five years and, subject to the provisions of this Schedule, he shall be eligible for re-appointment to the office.

4.(1) Where the Commissioner is -

(a) nominated as a member of the Senate;

(b) elected as a member of the House of Assembly or a local authority,

he shall thereupon cease to be the Commissioner.

(2) A person who is for the time being -

(a) a member of either House of Parliament;

(b) an elected local government member, shall, while he is so entitled or is such a member, be disqualified from holding the office of Commissioner.

5. The Commissioner shall not hold any other office or employment in respect of which emoluments are payable.

6. There shall be paid to the Commissioner, out of moneys provided from the Consolidated Fund, such remuneration and allowances for expenses as the Minister, with the consent of the Minister for Finance, may from time to time determine.

7. The Minister -

(a) shall, with the consent of the Minister for Finance, make and carry out, in accordance with its terms, a scheme or schemes for the granting of pensions, gratuities or other allowances on retirement or death to or in respect of persons who have held the office of Commissioner;

Section III

(b) may, with the consent of the Minister for Finance, at any time make and carry out, in accordance with its terms, a scheme or schemes amending or revoking a scheme under this paragraph, and a scheme under this paragraph shall be laid before each House of Parliament as soon as may be after it is made and, if a resolution annulling the scheme is passed by either such House within the next twenty-one days on which that House has sat after the scheme is laid before it, the scheme shall be annulled accordingly, but without prejudice to the validity of anything previously done thereunder.

8.(1) The Minister may appoint to be members of the staff of the Commissioner such number of persons as may be determined from time to time by the Minister, with the consent of the Minister for Finance.

(2) Members of the staff of the Commissioner shall be public officers.

(3) The functions of the Commissioner under this Act may be performed during his temporary absence by such member of the staff of the Commissioner as he may designate for that purpose.

9.(1) The Commissioner shall keep in such form as may be approved of by the Minister, with the consent of the Minister for Finance, all proper and usual accounts of all moneys received or expended by him and all such special accounts (if any) as the Minister, with the consent of the Minister for Finance, may direct.

(2) Accounts kept in pursuance of this paragraph in respect of each year shall be submitted by the Commissioner in the following year on a date (not later than a date specified by the Minister) to the Auditor-General for audit and, as soon as may be after the audit, a copy of those accounts, or of such extracts from those accounts as the Minister may specify, together with the report of the Auditor-General on the accounts, shall be presented by the Commissioner to the Minister who shall cause copies of the documents presented to him to be laid before each House of Parliament.

Barbados – NONE

Belize – NONE

Dominica, Grenada, St. Kitts and Nevis – NONE

St. Lucia* – LIMITED (GOOD) – Clear articulation of powers and responsibility of the oversight authority. With appointment at the sole discretion of the Head of State and strong entrenchment provisions, independence of decision-making is assured.
[Privacy and Data Protection Bill, 2007]

6. (1) Subject to subsection (2), there shall be a Data Protection Commissioner who shall be appointed by the Governor General after consultation with the Prime Minister and the Leader of the Opposition.

(2) A person is not qualified to hold office as Commissioner if he or she-
(a) is a Minister, Parliamentary Secretary, or a Member of the House of Assembly; or
(b) is a judge or magistrate; or
(c) is public officer; or
(d) is a member of a local authority; or
(e) has a financial or other interest in any enterprise or activity which is likely to affect the discharge of his or her functions as a Commissioner; or
(f) is an undischarged bankrupt; or
(g) has at any time been convicted of any offence involving dishonesty.

Section III

(3) The Commissioner shall be assisted by such public officers as may be necessary who shall be under the administrative control of the Commissioner.

(4) The Commissioner shall not hold any other office of emolument whether in the public service or otherwise and shall not engage in any other occupation for reward.

(5) The Prime Minister shall, after he or she has consulted the Leader of the Opposition, appoint a person who is qualified to be appointed as a temporary Commissioner if –

(a) the Commissioner resigns or if his office is otherwise vacant;
(b) the Commissioner is for any reason unable to perform the functions of his office
(c) the Commissioner considers it necessary, on a temporary basis, not to carry out any of his or her functions because of such circumstances, that were he a judge of the High Court, he would abstain

and any person so appointed shall cease to be a temporary Commissioner when a Commissioner is appointed to fill the vacancy or, as the case may be, when the Commissioner who was unable to perform the functions of his or her office resumes those functions or, in the case of a temporary purpose, the temporary Commissioner has performed the function assigned to him or her.

(6) The appointment of a temporary Commissioner for a temporary purpose as provided in subsection (3) (b) and (c) shall be exercised only on a certificate signed by the Commissioner to the effect that, in his or her opinion, it is necessary for the due conduct of the business of the Commissioner under this Act, that a temporary Commissioner be appointed.

7. (1) The Commissioner shall have a distinct legal personality and shall be capable, subject to the provisions of this Act, of entering into contracts, of acquiring, holding and disposing of any kind of property for the purposes of his or her functions, of suing and being sued, and of doing all such things and entering into all such transactions as are incidental or conducive to the exercise or performance of his or her functions under this Act. 9

(2) Any document purporting to be an instrument made or issued by the Commissioner and signed by him or her shall be received in evidence and shall, until the contrary is proved, be deemed to be an instrument made or issued by the Commissioner.

8. (1) The Commissioner shall hold office for a term not exceeding five years and shall be eligible for reappointment on the expiration of his or her term of office.

(2) Subject to the provisions of subsection (2), the Commissioner vacates his or her office-

(a) at the expiration of the term for which he or she was appointed;
(b) if he or she becomes disqualified by virtue of subsection 6(2); or
(c) if he or she is appointed to any other office of emolument or engages in any other occupation for reward;

(3) The Commissioner shall not be removed from his or her office except by the Governor General after consultation with the Prime Minister and the Leader of the opposition on the ground of inability to perform the functions of his or her office, whether arising from infirmity of body or mind or any other cause, or misbehaviour.

9. No action or other proceeding for damages shall be instituted against a Commissioner for an act done in good faith in the performance of a duty or in the exercise of a power or discretion under this Act.

Section III

10. The Commissioner may delegate any of his or her investigating and enforcement powers conferred upon him or her by this Act to any authorized officer and to any police officer designated for that purpose by the Commissioner.

11. In the exercise of his or her functions under this Act the Commissioner shall act independently and shall not be subject to the direction or control of any other person or authority.

12. The Commissioner shall-

(a) ensure compliance with this Act and the Regulations;
(b) create and maintain a register of data controllers;
(c) exercise control on all data processing activities and either of his or her own motion or at the request of a data subject, verify whether the processing of data is carried on in accordance with the provisions of this Act or the Regulations;
(d) instruct the data controller to take such measures as may be necessary to ensure that the processing of data is in accordance with this Act or the Regulations; and
(e) investigate reports and claims from data subjects or associations representing data subjects on violations of this Act or the Regulations and take remedial action as the Commissioner deems necessary or as may be prescribed under this Act, and to inform the data subjects or associations of the outcome;
(f) issue such directions or public statements as may be required of the Commissioner for the purposes of this Act;
(g) take such measures as may be necessary so as to bring the provisions of this Act to the knowledge of the general public, the provisions of this Act;
(h) promote by education and publicity, an understanding and acceptance of the data protection principles and of the objects of those principles;
(i) advise the Government on any legislative measures that are required to be taken relating to this privacy and data protection;
(j) either of his or her own motion or upon request, report to the Minister as the need arises on any matter affecting the privacy of a data subject, including any recommendations relating to the need for or the desirability of, taking legislative, administrative or other action to give protection, or better protection, to the privacy of the da`ta subject;
(k) collaborate with supervisory authorities of other countries to the extent necessary for the performance of his or her duties, in particular by exchanging all useful information, in accordance with any convention to which Saint Lucia is a party or any other international obligation of Saint Lucia;
(l) generally monitor compliance by governmental and non-governmental bodies with the provisions of this Act;
(m) prepare and issue or approve, in consultation with the Minister, appropriate codes of practice or guidelines for the guidance of business persons and institutions handling personal data;
(n) undertake research into and monitor developments in data processing and computer technology to ensure that any adverse effects of such developments on the privacy of data subjects are minimized, and include the results of such research and monitoring, if any, in the annual report required pursuant to section 60;
(o) provide advice, with or without request, to a Minister or a public authority on any matter relevant to the operation of this Act and report to the Minister as the need arises on the desirability of the acceptance by Saint Lucia of any international instrument relating to the privacy of data subjects;
(p) do any thing incidental or conducive to the performance of any of the preceding functions; and
(q) exercise and perform such other functions as are conferred or imposed on the Commissioner by or under this Act, or any other enactment.

Section III

13. (1) The Commissioner and every authorized officer shall take the oath specified in the Schedule before the Governor General.

(2) A person who is or has been the Commissioner, an officer of the Commissioner's staff or an agent of the Commissioner shall not make use of or divulge, either directly or indirectly, any data obtained as a result of the exercise of a power or in the performance of a duty under this Act, except –

(a) in accordance with this Act or any other enactment; or
(b) as authorized by the order of a Court.

(3) A person who, without lawful excuse, contravenes subsection (2), commits an offence and is liable on conviction to a fine not exceeding twenty five thousand dollars or to imprisonment for a term not exceeding six months or to both.

14. The Commissioner shall have power, for the purpose of carrying out his or her functions to do all such acts as appear to him or her to be requisite, advantageous or convenient for, or in connection with the carrying out of these functions.

St. Vincent and the Grenadines – POOR – particularly with regard to clause 17 (2) which suggests that the Commissioner is a public servant, and Clause 19 where the role of the Commissioner is not the full time job of the incumbent. This may lead to conflicts of interest if the scope is widened beyond the public service. The powers of investigation are also weak.

16. (1) For the purposes of this Act, there is hereby established the office of Privacy Commissioner.

(2) The Privacy Commissioner shall be appointed by the Governor-General upon consultation with the Public Service Commission, subject to such terms and conditions as may be specified in the instrument of appointment.

17. (1) A person appointed as Privacy Commissioner shall hold office during good behaviour for a period of three years and shall, at the expiration of such period, be eligible for reappointment.

(2) A person appointed as Privacy Commissioner may resign from office by writing under his or her hand addressed to the Governor-General and shall in any case vacate office on attaining the age of sixty-five years.

(3) The Privacy Commissioner may be removed from office only for inability to discharge the functions of office (whether arising from infirmity of body or mind or any other cause) or for misbehaviour.

18. (1) No person shall be qualified for appointment to the office of Privacy Commissioner if that person –

(a) is a Member of Parliament;
(b) is a member of a local authority;
(c) is an undischarged bankrupt; or
(d) has at any time been convicted of any offence involving dishonesty or moral turpitude.

(2) The Privacy Commissioner shall vacate office if any circumstances arise that, if he or she were not Privacy Commissioner, would cause him or her to be disqualified for appointment as such, by virtue of subsection (1) of this section.

19. A person appointed as Privacy Commissioner shall not necessarily be a full-time officer and may be employed in any other capacity during any period in which the person holds office as Privacy Commissioner.

Section III

20. (1) Where -

(a) a vacancy arises in the office of Privacy Commissioner; or

(b) by reason of illness, absence from the country or other sufficient cause, a person appointed as Privacy Commissioner is unable to perform his or her functions under this Act,

the Governor-General may, upon consultation with the Public Service Commission, appoint a suitable person to act in that office or perform those functions, as the case may be.

21. (1) The functions of the Privacy Commissioner shall be -

(a) to monitor compliance by public authorities of the provisions of this Act;

(b) to provide advice to public authorities on their obligations under the provisions, and generally on the operation, of this Act;

(c) to receive and investigate complaints about alleged violations of the privacy of persons and in respect thereof may make reports to complainants;

(d) to inquire generally into any matter, including any enactment or law, or any practice, or procedure, whether governmental or non-governmental, or any technical development, if it appears to the Commissioner that the privacy of the individual is being, or may be, infringed thereby;

(e) for the purpose of promoting the protection of individual privacy, to undertake educational programmes on the Commissioner's own behalf or in co-operation with other persons or authorities acting on behalf of the Commissioner;

(f) to make public statements in relation to any matter affecting the privacy of the individual or of any class of individuals;

(g) to receive and invite representations from members of the public on any matter affecting the privacy of the individual;

(h) to consult and co-operate with other persons and bodies concerned with the privacy of the individual;

(i) to make suggestions to any person in relation to any matter that concerns the need for , or the desirability of, action by that person in the interests of the privacy of the individuals;

(j) to undertake research into, and to monitor developments in, data processing and computer technology to ensure that any adverse effects of such developments on the privacy of individuals are minimised, and to report to the Minister the results of such research and monitoring;

(k) to examine any proposed legislation including subordinate legislation or proposed policy of the Government that the Commissioner considers may affect the privacy of individuals, and to report to the Minister the results of that examination;

(l) to report with or without request to the Minister from time to time on any matter affecting the privacy of the individual, including the need for, or desirability of, taking legislative, administrative, or other action to give protection or better protection to the privacy of the individual;

(m) to report to the Minister from time to time on the desirability of the acceptance, by Saint Vincent and the Grenadines of any international instrument relating to the privacy of the individuals;

(n) to gather such information as in the opinion of the Commissioner will assist the Commissioner in discharging the duties and performing the functions of the Commissioner under this Act;

(o) to receive complaints from any decision of a public authority pursuant to section 15 (4) refusing an application for the amendment of information;

(p) to do anything incidental or conducive to the performance of any of the preceding functions; and

(q) to exercise and perform such other functions, powers, and duties as are conferred or imposed on the Commissioner by or under this Act or any other enactment.

Section III

22. (1) There shall be appointed such officers and employees as may be necessary to enable the Privacy Commissioner to discharge the duties and perform the functions of such Commissioner under this Act.

(2) Parliament shall appropriate annually, for the use of the Privacy Commissioner, such sums of money as may be necessary for the proper exercise, performance and discharge, by the Commissioner, of his or her powers, duties and functions under this Act.

…..

31. The Commissioner shall, as soon as practicable after the thirty-first of December of each year, prepare a report on the activities of the office during that year and cause a copy of the report to be laid before Parliament.

32. The Commissioner and every person acting on behalf or under the direction of the Commissioner who receives or obtains information relating to any investigation under this Act or any other Act of Parliament shall, with respect to the use of that information, satisfy any security requirements applicable to, and take any oath of secrecy required to be taken by, persons who normally have access to and use of that information.

33. Subject to this Act, the Commissioner and every person acting on behalf or under the direction of the Commissioner shall not disclose any information that comes to their knowledge in carrying out duties and performing functions under this Act.

34. (1) Notwithstanding the provisions of section 37, no criminal or civil proceedings lie against the Commissioner, or against any person acting on behalf or under the direction of the Commissioner, for anything done, reported or said in good faith in the course of the exercise or performance or purported exercise, discharge, or performance of any power, duty or function of the Commissioner under this Act.

(2) For the purpose of any law relating to libel or slander,

(a) anything said, any information supplied or any document or thing produced in good faith in the course of an investigation carried out by or on behalf of the Commissioner under this Act is absolutely privileged; and

(b) any report made in good faith by the Commissioner under this Act is absolutely privileged.

35. (1) No person shall obstruct the Commissioner or any person acting on behalf or under the direction of the Commissioner in the discharge and performance of the Commissioner's duties and functions under this Act.

(2) Every person who contravenes this section is guilty of an offence and liable on summary conviction to a fine not exceeding five thousand dollars.

Jamaica – NONE

St. Kitts and Nevis – LIMITED – Draft legislation is reported to be in preparation before presentation to Parliament, and is as such confidential. Copies of the draft were not available for assessment.

Section III

Trinidad and Tobago* – LIMITED (GOOD) – Clear articulation of powers and responsibility of the oversight authority. However with appointment by the Head of State at the advice of the Cabinet, there is the potential that independence is threatened, despite strong entrenchment provisions. Further specification that the Commissioner is an attorney-at-law is not in alignment with best practice.

7. There is hereby established a body to be known as the Office of the Data Commissioner.

8. (1) There shall be a Data Commissioner who shall be the head of the Office of the Data Commissioner and who shall be appointed by the President and who shall possess the qualifications and experience set out in subsection (2).

(2) A person appointed to be the Data Commissioner under subsection (1) shall be an attorney-at-law within the meaning of the Legal Profession Act with at least ten years standing at the bar and shall have training or experience in economics, finance, information security, technology, audit or human resource management.

(3) The Data Commissioner shall be a corporation sole.

(4) A person appointed under subsection (1) shall hold office for five years and may be reappointed.

(5) A person appointed under subsection (1) shall, before he performs the functions of Data Commissioner, take and subscribe to the oath of office set out in the Schedule.

9. (1) The Commissioner shall monitor the administration of this Act to ensure its purposes are achieved.

(2) In carrying out his powers under subsection (1), the Commissioner may–

(a) conduct audits and investigations to ensure compliance with any provision of this Act;

(b) offer comment on the privacy protection implications of proposed legislative schemes or government programmes and receive representations from the public concerning data protection and privacy matters;

(c) after hearing the representations of the head of a public authority or an organization subject to a mandatory code of conduct and who may be engaged in processes that may be in contravention of this Act, order the public authority or organization to cease collection practices or destroy collections of personal information that contravene this Act;

(d) authorize the collection of personal information otherwise than directly from the individual in appropriate circumstances;

(e) make orders regarding the reasonableness of fees required by an organization subject to this Act;

(f) authorize data matching by a public authority or public authorities;

(g) make orders, including such terms and conditions as the Commissioner considers appropriate, following an appeal or complaint filed by an individual pursuant to section 58 or 76;

(h) make orders regarding compliance with the General Privacy Principles set out in section 6 by a public authority or an organization subject to a mandatory code of conduct;

(i) hold such property as is by this Act vested in him, as well as such property as may from time to time–

(i) by virtue of any other written law; or

(ii) in any other way,

be or may become vested in him;

(j) with the permission of the President acquire, purchase, take, hold and enjoy movable and immovable property of every description, convey, assign, surrender and yield up, mortgage, demise, reassign, transfer or otherwise dispose of, or deal with any movable or immovable property vested in the Commissioner upon such terms as the Commissioner seems fit;

(k) accept surrenders, assignments or re-conveyances and to exchange any property and enter into contracts;

(l) publish guidelines regarding compliance with the Act, including but not limited to guidelines on the development of industry codes of conduct, firm compliance policies, procedures for handling complaints, guidelines dealing with conflict of interest for industry bodies or individuals who mediate or deal with complaint resolution, guidelines dealing with security of information and information systems, and guidelines for information sharing agreements or data matching agreements;

(m) exercise his corporate powers in relation thereto in such manner as he thinks fit, subject always to any special or general directions as the President may from time to time specify; and

(n) exercise such other powers as may be assigned to him under any other written law.

10. The Commissioner appointed under section 8 shall–

(a) promote the development of codes of conduct for guidance as to good practice;

(b) promote the adherence to good practices by persons subject to this Act;

(c) disseminate information about this Act;

(d) monitor compliance with this Act;

(e) co-operate with counterparts in other jurisdictions to promote the protection of personal privacy in the public and private sectors;

(f) carry out special studies or research regarding privacy or related issues either upon his own initiative or upon the request of the President;

(g) bring to the attention of the head of the public authority or organization subject to a mandatory code of conduct any failure to meet the standards imposed by the General Privacy Principles set out in section 6 or the responsibilities established by Part III and Part IV of this Act;

(h) issue public reports on the status of compliance with this Act;

(i) review and approve privacy impact assessments as required by this Act; and

(j) exercise such other functions that may be assigned to him under any other written law.

11. (1) There shall be a Deputy Data Commissioner who shall be appointed by the President and who shall possess the same qualifications and experience required for the Data Commissioner under section 8.

(2) The Deputy Data Commissioner shall hold office for five years and may be reappointed.

(3) The Deputy Data Commissioner may, in the absence or incapacity of the Data Commissioner, act in his place.

(4) Where the post of Data Commissioner is vacant the Deputy Data Commissioner may act as the Data Commissioner until such time as a Data Commissioner is appointed to the vacant post.

(5) In the absence or incapacity of the Deputy Data Commissioner, the President may appoint an acting Deputy Data Commissioner.

Section III

12. (1) The Commissioner or Deputy Data Commissioner may be removed from office only for cause, including misconduct in relation to his duties or physical or mental inability to fulfil the responsibilities of the office.

(2) The Commissioner or Deputy Data Commissioner may at any time resign his office by letter addressed to the President.

13. Section 141 of the Constitution [Remuneration] shall apply to the offices of the Commissioner and the Deputy Data Commissioner.

14. (1) The Corporation shall have a seal which shall be kept in the custody of the Commissioner and shall be judicially noticed as such.

(2) The seal of the Corporation may be affixed to documents and instruments in the presence of the Commissioner and shall be attested by the signature of the Commissioner and the signature shall be sufficient evidence that the seal was duly and properly affixed and is the lawful seal of the Corporation.

(3) All documents, other than those required by law to be under seal made by, and all decisions of the Corporation may be signified under the hand of the Commissioner.

(4) Notwithstanding the provisions of the Conveyancing and Law of Property Act and the Real Property Act relating to the matters thereunder required to be performed and to the mode of their performance prior to the registration of a Deed, document or other instrument, the affixing of the seal of the Corporation and the signing by the Commissioner in the manner set out in subsection (2) shall be, and shall be taken as, sufficient evidence for the purposes of those Acts of the due execution by the Corporation of any Deed, document or other instrument.

15. (1) The office of the Corporation shall be situated at the Office of the Data Commissioner.

(2) Service upon the Commissioner of any notice, order or other document shall be effected by delivering the same or by sending it by registered post addressed to the Commissioner at the office of the Corporation.

16. (1) Any document required to be executed by the Corporation shall be deemed to be duly executed if signed–

(a) by the Commissioner; or

(b) outside Trinidad and Tobago, by the person or persons authorized by the Commissioner so to sign, but in such case the instrument so authorizing such person or persons shall be attached to and form part of the document.

(2) Any cheque, bill of exchange or order for the payment of money required to be executed by the Commissioner shall be deemed to be duly executed if signed by a person or persons authorized to do so by the Commissioner.

17. (1) The Commissioner may employ such persons as he considers necessary for the due and efficient performance of his duties and functions under this Act on such terms and conditions as are agreed between the Commissioner and the person and subject to such maximum limit of remuneration as the Minister may determine.

(2) Subject to subsection (3) and the approval of the appropriate Service Commission or Statutory Authority and with the consent of the officer, any officer in the public service or a Statutory Authority may be seconded to the service of the Office of the Data Commissioner.

…

Section III

18. (1) Subject to subsection (2), the Commissioner may authorize any person to exercise or perform, subject to such restrictions or limitations as the Commissioner may specify, any powers, duties or functions of the Commissioner.

(2) The Commissioner may delegate to only the Deputy Data Commissioner responsibilities regarding review of personal information that deals with matters that may be exempt from disclosure pursuant to sections 24 to 26 of the Freedom of Information Act.

…

20. (1) Where the Data Commissioner is conducting an audit or enquiry into the practices of a public authority for the purposes of ensuring compliance with the General Privacy Principles set out in Part I, or determining an appeal pursuant to Part III, the Commissioner may–

(a) with the permission of the head of the public authority or on application for a warrant under subsection (4), enter and inspect any premises occupied by a public authority for the purposes of an audit or enquiry;

(b) require the production of any document or record relevant to the enquiry that is in the custody or control of a public authority.

(2) The Commissioner shall not retain any information obtained from an audit or enquiry under subsection (1) beyond the period for which it is required.

(3) The Commissioner may exercise his powers under this section with respect to Parliament, a Joint Select Committee of Parliament or a committee of either House of Parliament, the Cabinet, the Court of Appeal, the High Court, the Industrial Court, the Tax Appeal Board or any court of summary jurisdiction, the Tobago House of Assembly, the Executive Council of the Tobago House of Assembly only with the consent of the Speaker of the House or the President of the Senate, the Head of the Cabinet, the Chief Justice, the Presiding Officer or the Head of the Executive Council, as the case may be.

(4) Where the head of a public authority refuses to–

(a) allow the Data Commissioner or any person acting for or under him to enter and inspect premises under subsection (1)*(a)*, the Data Commissioner shall, where he believes that such entry is necessary, apply to a Magistrate for a warrant to so enter and inspect; or

(b) produce a document or record under subsection (1)*(b)*, the Data Commissioner shall, where he believes the request to be reasonable, apply to the Court for an Order requiring the public authority to produce such documents.

(5) Subsection (4) shall not apply to any authority referred to in subsection (3).

21. (1) Where the Commissioner is conducting an audit or enquiry into the compliance practices of a person subject to the provisions of an enforceable code of conduct pursuant to Part IV of this Act, the Commissioner may, pursuant to the authority provided under subsection (2) by–

(a) an Order of the Court, require the production of any document or record that is in the custody or control of a person subject to an enforceable code of conduct; or

(b) a warrant, enter and inspect any premises occupied by a person subject to an enforceable code of conduct for the purposes of an audit or enquiry.

(2) Where a private enterprise refuses to allow the Data Commissioner or any person acting for or under him to enter and inspect premises under subsection (1)*(a)*, the Data Commissioner may apply to a Magistrate for a warrant to so enter and inspect.

Section III

(3) Where a private enterprise refuses to produce a document or record under subsection (1)*(b)*, the Data Commissioner may apply to the Court for an Order requiring the public authority to produce such documents.

(4) The Commissioner shall not retain any information obtained from an audit or enquiry under subsection (1) beyond the period for which it is required.

22. (1) All expenses of the Office of the Data Commissioner shall be met out of moneys provided by Parliament.

(2) All revenues of the Office of the Data Commissioner shall be paid into the Consolidated Fund.

(3) The accounts of the Office of the Data Commissioner shall be audited by the Auditor General in accordance with the provisions of the Exchequer and Audit Act.

23. A statement made to or an answer given by a person during an investigation or enquiry by the Commissioner is inadmissible as evidence in court or any other proceeding, except in–

(a) a prosecution for perjury in respect of sworn testimony;
(b) a prosecution for an offence under this Act; or
(c) an application for judicial review or an appeal from a decision with respect to that application.

24. Anything said in information supplied or any data produced by a person during an investigation or enquiry by the Commissioner is privileged in the same manner as if the investigation or enquiry were a proceeding in a court.

25. (1) The Commissioner and anyone acting for or under the direction of the Commissioner shall not disclose any information obtained in performing their duties, powers and functions under this Act.

(2) Notwithstanding subsection (1), the Commissioner may disclose or may authorize anyone acting for or under the direction of the Commissioner, to disclose information–

(a) necessary to conduct an investigation, audit or enquiry under this Act or establish grounds for findings and recommendations contained in a report under the Act; or

(b) in the course of a prosecution or an appeal from, or judicial review of, a decision of the Commissioner.

26. Proceedings shall not lie against the Commissioner or a person acting for or under the direction of the Commissioner for anything done, reported or said in good faith in the exercise or performance or the intended exercise or performance of a duty, power or function under this Part.

27. (1) The Commissioner shall submit a report annually to Parliament on the activities of the Office of the Data Commissioner for the previous year commencing one year after the coming into operation of this Act.

(2) The Commissioner may submit a special report to Parliament at any time commenting on any matters within the scope, duties and functions of the Commissioner where the matter is of such urgency or importance that it should not be deferred to the time of the next annual report to Parliament.

28. The Data Commissioner shall by Order publish a list of countries which have comparable safeguards for personal information as provided by this Act.

Section III

Whistleblower protection

97. An employer whether or not a public authority, shall not dismiss, suspend, demote, discipline, harass or otherwise disadvantage an employee or deny that employee a benefit, because–

(a) the employee acting in good faith, and on the basis of reasonable belief has–

(i) notified the Commissioner that the employer or any other person has contravened or is about to contravene this Act;

(ii) done or stated the intention of doing anything that is required to be done in order to avoid having any person contravene this Act; or

(iii) refused to do or stated the intention of refusing to do anything that is in contravention of this Act; or

(b) the employer believes that the employee will do anything described in paragraph *(a).*

International Examples and Regional Harmonization

United Nations

Guidelines Concerning Computerized Personal Data Files (1990)

Supervision and Sanctions

UN (1990) Prinicple 8 – The law of every country shall designate the authority which, in accordance with its domestic legal system, is to be responsible for supervising observance of the principles set forth above. This authority shall offer guarantees of impartiality, independence vis-a-vis persons or agencies responsible for processing and establishing data, and technical competence. In the event of violation of the provisions of the national law implementing the aforementioned principles, criminal or other penalties should be envisaged together with the appropriate individual remedies.

European Union

Article 28 – Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

These authorities shall act with complete independence in exercising the functions entrusted to them.

2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

3.2.3 Regulatory Empowerment

International Best Practices and Regional Trends:

- The framework clearly underscores the nature of the forms of interaction between these persons and the oversight body.
- The framework provides for cooperation in the instance of investigation or enquiry by the oversight body.
- The framework provides for enforcement actions to be taken against errant collectors of information.

Regional Examples

Antigua and Barbuda – NONE

Bahamas – GOOD – Clear articulation of investigative powers. Clear outline of process by which Commissioner engages data controllers. The process is backed up by a regime of offences.

15. (1) The Commissioner may investigate, or cause to be investigated, whether any of the provisions of this Act have been, are being or are likely to be contravened by a data controller or a data processor in relation to an individual either where the individual complains to him of a contravention of any of those provisions or he is otherwise of the opinion that there may be such a contravention.

(2) Where a complaint is made to the Commissioner under subsection (1), the Commissioner shall -

(a) investigate the complaint or cause it to be investigated, unless he is of the opinion that it is frivolous or vexatious; and

(b) as soon as may be, notify the individual concerned in writing of his decision in relation to the complaint and that the individual may, if aggrieved by his decision, appeal against the decision under section 24.

(3) If the Commissioner is of the opinion that a data controller or a data processor, has contravened or is contravening a provision of this Act (other than a provision the contravention of which is an offence), the Commissioner may, by notice in writing (referred to in this Act as an enforcement notice) served on the person, require him to take such steps as are specified in the notice within such time as may be so specified to comply with the provision concerned.

(4) Without prejudice to the generality of subsection (3), if the Commissioner is of the opinion that a data controller has contravened section 6, the relevant enforcement notice may require him -

(a) to rectify or erase any of the data concerned; or

(b) to supplement the data with such statement relating to the matters dealt with by them as the Commissioner may approve; and as respects data that are inaccurate or not kept up to date, if he supplements them as aforesaid, he shall be deemed not to be in contravention of subsection (1)(b) of section 6.

16.(1) The Commissioner may issue an enforcement notice which shall -

(a) specify any provision of this Act that, in the opinion of the Commissioner, has been or is being contravened and the reasons for his having formed that opinion; and

Section III

(b) subject to subsection (2), state that the person concerned may appeal to the Court under section 24 against the requirement specified in the notice within twenty-one days from the service of the notice on him.

(2) Subject to subsection (3), the time specified in an enforcement notice for compliance with a requirement specified therein shall not be expressed to expire before the end of the period of twenty-one days specified in subsection (1) (b) and, if an appeal is brought against the requirement, the requirement need not be complied with and subsection (6) shall not apply in relation thereto, pending the determination or withdrawal of the appeal.

(3) If the Commissioner -

(a) by reason of special circumstances, is of the opinion that a requirement specified in an enforcement notice should be complied with urgently; and

(b) such enforcement notice includes a statement to that effect,

subsections (1)(b) and (2) shall not apply in relation to the notice, but the notice shall contain a statement of the effect of the provisions of section 24 (other than subsection (2)) and shall not require compliance with the requirement before the end of the period of seven days beginning on the date on which the notice is served.

(4) On compliance by a data controller with a requirement under subsection (4) of section 15, he shall, as soon as may be and in any event not more than forty days after such compliance, notify -

(a) the data subject concerned; and

(b) any person (where the Commissioner considers it reasonably practicable to do so) to whom the data were disclosed during the period beginning twelve months before the date of the service of the enforcement notice concerned and ending immediately before such compliance, of the rectification, erasure or statement concerned, if such compliance materially modifies the data concerned.

(5) The Commissioner may cancel an enforcement notice and, if he does so, shall notify in writing the person on whom it was served accordingly.

(6) A person who, without reasonable excuse, fails or refuses to comply with a requirement specified in an enforcement notice shall be guilty of an offence.

17.(1) The Commissioner may, subject to the provisions of this section, prohibit the transfer of personal data from The Bahamas to a place outside The Bahamas, in such cases where there is a failure to provide protection either by contract or otherwise equivalent to that provided under this Act.

(2) In determining whether to prohibit a transfer of personal data under this section, the Commissioner shall also consider whether the transfer would be likely to cause damage or distress to any person and have regard to the desirability of facilitating international transfers of data.

(3) A prohibition under subsection (1) shall be effected by the service of a notice (referred to in this Act as a prohibition notice) on the person proposing to transfer the data concerned.

(4) A prohibition notice shall -

(a) prohibit the transfer concerned either absolutely or until the person aforesaid has taken such steps as are specified in the notice for protecting the interests of the data subjects concerned;

(b) specify the time when it is to take effect;

(c) specify the grounds for the prohibition; and

Section III

(d) subject to subsection (6), state that the person concerned may appeal to the Court under section 24 against the prohibition specified in the notice within twenty-one days from the service of the notice on him.

(5) Subject to subsection (6), the time specified in a prohibition notice for compliance with the prohibition specified therein shall not be expressed to expire before the end of the period of the twenty-one days specified in subsection (4) (d) and, if an appeal is brought against the prohibition, the prohibition need not be complied with and subsection (10) shall not apply in relation thereto, pending the determination or withdrawal of the appeal.

(6) If the Commissioner -

(a) by reason of special circumstances, is of the opinion that a prohibition specified in a prohibition notice should be complied with urgently; and

(b) such prohibition notice includes a statement to that effect,

subsections (4) (d) and (5) shall not apply in relation to the notice but the notice shall contain a statement of the effect of the provisions of section 24 (other than subsection (2)) and shall not require compliance with the prohibition before the end of the period of seven days beginning on the date on which the notice is served.

(7) The Commissioner may cancel a prohibition notice and, if he does so, shall notify in writing the person on whom it was served accordingly.

(8) This section shall not apply to a transfer of data if the transfer of the data or the information constituting the data is required or authorised by or under any enactment, or required by any convention or other instrument imposing an international obligation on The Bahamas, or otherwise made pursuant to the consent (express or implied) of the data subjects.

(9) This section applies, with any necessary modifications, to a transfer of information from The Bahamas to a place outside The Bahamas for conversion into personal data as it applies to a transfer of personal data from The Bahamas to such a place; and in this subsection "information" means information (not being data) relating to a living individual who can be identified from it.

(10) A person who, without reasonable excuse, fails or refuses to comply with a prohibition specified in a prohibition notice shall be guilty of an offence.

18.(1) The Commissioner may, by notice in writing (referred to in this Act as an information notice) served on a person, require the person to furnish to him in writing within such time as may be specified in the notice such information in relation to matters specified in the notice as 1 is necessary or expedient for the performance by the Commissioner of his functions.

(2) Subject to subsection (3) -

(a) an information notice shall state that the person concerned may appeal to the Court under section 24 against the requirement specified in the notice within twenty-one days from the service of the notice on him; and

(b) the time specified in the notice for compliance with a requirement specified therein shall not be expressed to expire before the end of the period of twenty-one days specified in paragraph (a) and, if an appeal is brought against the requirement, the requirement need not be complied with and subsection (5) shall not apply in relation thereto, pending the determination or withdrawal of the appeal.

(3) If the Commissioner -

(a) by reason of special circumstances, is of the opinion that a requirement specified in an information notice- should be complied with urgently; and

Section III

(b) such information notice includes a statement to that effect,

subsection (2) shall not apply in relation to the notice, but the notice shall contain a statement of the effect of the provisions of section 24 (other than subsection (2)) and shall not require compliance with the requirement before the end of the period of seven days beginning on the date on which the notice is served.

(4) No enactment or rule of law prohibiting or restricting the disclosure of information shall preclude a person from furnishing to the Commissioner any information that is necessary or expedient for the performance by the Commissioner of his functions and this subsection shall not apply to information that in the opinion of the Minister or the Minister for National Security is, or at any time was, kept for the purpose of safeguarding the security of The Bahamas or information that is privileged from disclosure in proceedings in any court.

(5) A person who, without reasonable excuse, fails or refuses to comply with a requirement specified in an information notice or who in purported compliance with such a requirement furnishes information to the Commissioner that the person knows to be false or misleading in a material respect shall be guilty of an offence.

19.(1) In this section "authorised officer" means a person authorised in writing by the Commissioner to exercise the powers conferred by this section, for the purposes of this Act.

(2) Where a Magistrate is satisfied by evidence on oath that there is reasonable cause to believe that for the purpose of obtaining any information that is necessary or expedient for the performance by the Commissioner of his functions, he may grant a warrant directed to an authorised officer to -

(a) enter, at all reasonable times, premises that he reasonably believes to be occupied by a data controller or a data processor, inspect the premises and any data therein (other than data consisting of information specified in subsection (4) of section 18) and inspect, examine, operate and test any data equipment therein;

(b) require any person on the premises, being a data controller, a data processor or an employee of either of them, to disclose to the officer any such data and produce to him any data material (other than data material consisting of information so specified) that is in that person's power or control and to give to him such information as he may reasonably require in regard to such data and material;

(c) either on the premises or elsewhere, inspect and copy or extract information from such data, or inspect and copy or take extracts from such material; and

(d) require any person mentioned in paragraph (b) to give to the officer such information as he may reasonably require in regard to the procedures employed for complying with the provisions of this Act, the sources from which such data are obtained, the purposes for which they are kept, the persons to whom they are disclosed and the data equipment in the premises.

(3) A person who obstructs or impedes an authorised officer in the exercise of a power, or without reasonable excuse does not comply with a requirement under this section, or who in purported compliance with such a requirement gives information to an authorised officer that he knows to be false or misleading in a material respect shall be guilty of an offence.

Barbados – NONE

Belize – NONE

Dominican Republic – NONE

Dominica, Grenada – NONE

Section III

Jamaica – NONE

St. Kitts and Nevis – LIMITED – Draft legislation is reported to be in preparation before presentation to Parliament, and is as such confidential. Copies of the draft were not available for assessment.

St. Lucia*, – LIMITED (GOOD) – Clear articulation of investigative powers. Clear outline of process by which Commissioner engages data controllers in support of an investigation. The process is backed up by a regime of enforcement notifications and offences.

15. (1) The Commissioner may, by a written information notice served on any person, request that person to furnish to him or her in writing in the time specified-
    (a) access to personal data;
    (b) information about and documentation of the processing of personal data;
    (c) information related to the security of processing of personal data; and
    (d) any other information in relation to matters specified in the notice as is necessary or expedient for the performance by the Commissioner of his or her functions and exercise of his or her powers and duties under this Act.

(2) Where the information requested by the Commissioner is stored in a computer, disc, cassette, or on microfilm, or preserved by any mechanical or electronic device, the person named in the information notice shall produce or give access to the information in a form in which it can be taken away and in which it is visible and legible.

(3) A notice required or authorized by this Act to be served on or given to any person by the Commissioner may –
    (a) if that person is an individual, be served on him or her by;
        (i) delivering, personally to the person;
        (ii) sending it to the person by post addressed to the person at his or her usual or last known place of business; or
        (iii) leaving it for the person at or her last known place of business that place;
    (b) if that person is a body corporate or partnership, be served by –
        (i) sending it by post to the proper officer of the company at its principal office;
        (ii) addressing it to the proper officer of the partnership and leaving it at the office of the proper officer.

16. (1) Subject to subsection (2), the information notice specified in section 16 shall state-
    (a) that the person to whom the notice is addressed has a right of appeal under section 59 against the requirement specified in the notice within thirty days from the service of the notice on him or her; and
    (b) the time for compliance with a requirement specified in the information notice, which time shall not be expressed to expire before the end of the period of thirty days specified in paragraph (a).

(2) Where a notice of appeal against a decision made under section 16, is lodged with the Commissioner, the information required need not be furnished, and section 18 shall not apply in relation thereto, pending the determination or withdrawal of the appeal.

(3) Where the Commissioner considers that by reason of special circumstances the information is required urgently for the proper performance of his or her functions and exercise of his or her powers under this Act, the Commissioner may apply to a Judge in Chambers for communication of the information.

Section III

(4) A law in force in Saint Lucia or rule of law prohibiting or restricting the disclosure of information shall not preclude a person from furnishing to the Commissioner any information that is necessary or expedient for the performance by the Commissioner of his or her functions and this subsection shall not apply to information that in the opinion of the Minister or the Minister responsible for national security is, or at any time was, kept for the purpose of safeguarding the security of Saint Lucia or information that is privileged from disclosure in proceedings in any court.

17. (1) A person shall not, without reasonable excuse, fail or refuse to comply with a requirement specified in an information notice.

(2) A person shall not, in purported compliance with an information notice furnish information to the Commissioner that the person knows to be false or misleading in a material respect.

(3) A person who contravenes subsection (1) or (2) commits an offence and is liable shall commit an offence and shall be liable on summary conviction to a fine not exceeding twenty five thousand dollars or to imprisonment for a term not exceeding six months or to both.

(4) It is a defence for a person charged with an offence under subsection (1) or (2) to prove that he or she exercised all due diligence to comply with the information notice.

18. If the Commissioner cannot, pursuant to a request under section 16(1), obtain sufficient information in order to conclude that the processing of personal data is lawful, the Commissioner may prohibit the data controller from processing personal data in any other manner than by storing the personal data.

19. (1) The Commissioner may, on complaint by a data subject or at the Commissioner's instance, investigate, or cause to be investigated, whether any provisions of this Act or the Regulations have been, are being or are likely to be contravened by a data controller in relation to a data subject.

(2) Where a complaint is made to the Commissioner under subsection (1), the Commissioner shall –

(a) investigate the complaint or cause it to be investigated by an authorized officer, unless the Commissioner is of the opinion that it is frivolous or vexatious; and

(b) as soon as reasonably practicable, notify the data subject concerned in writing of his or her decision in relation to the complaint and that the data subject may, if aggrieved by the Commissioner's decision, appeal against the decision to the Court under section 59.

(3) Nothing in this Act precludes the Commissioner from receiving and investigating complaints that are submitted by a person authorized in writing by the data subject concerned to act on behalf of the data subject, and a reference to a data subject in any other section of this Act includes a reference to the person so authorized.

Power of Commissioner to issue enforcement notice

27. (1) Where the Commissioner is of the opinion that a data controller has contravened or is contravening a provision of this Act, other than a provision the contravention of which is an offence, the Commissioner may, subject to section 28, serve an enforcement notice on the data controller, requiring the data controller person to take such steps as are specified in the enforcement notice within such time as may be so specified to comply with the provision concerned.

Section III

28. (1) An enforcement notice shall be in writing and shall-
(a) specify the provision of this Act that, in the opinion of the Commissioner, the data controller has contravened or is contravening and the reasons for the Commissioner having formed that opinion; and
(b) specify the action which the Commissioner requires the data controller to take;
(c) subject to subsection (2), inform the data subject of his or her right of appeal pursuant to section 59 and the time within which the appeal must be lodged.

(2) An enforcement notice may, without prejudice to the generality of section 27 or subsection (1), require the data controller-
(a) to rectify or erase any of the data concerned; or
(b) to supplement the personal data with such statement relating to the matters dealt with by them as the Commissioner may approve;

and with respect to the personal data that is inaccurate or not kept up to date, if the data controller complies with paragraphs (a) or (b), the data controller shall be deemed not to be in contravention of the provision.

(3) Subject to subsection (5), the time specified in an enforcement notice for compliance with a requirement specified in the enforcement notice shall not be expressed to expire before the end of the period for appeal specified in section 59 and, if an appeal is brought against the requirement, the requirement need not be complied with and subsection (6) shall not apply in relation thereto, pending the determination or withdrawal of the appeal.

(5) If the Commissioner –
(a) by reason of special circumstances, is of the opinion that a requirement specified in an enforcement notice shall be complied with urgently; and
(b) the enforcement notice includes a statement to that effect,

subsections (1)(b) and (2) shall not apply in relation to the enforcement notice, but the notice shall contain a statement of the effect of the provisions of section 59, other than subsection (2), and shall not require compliance with the requirement before the end of the period of seven days beginning on the date on which the notice is served.

(4) On compliance by a data controller with a requirement under subsection (2) of section 25, the data controller shall, as soon as may be and in any event not more than thirty days after such compliance, notify –
(a) the data subject concerned; and
(b) any person, where the Commissioner considers it reasonably practicable to do so, to whom the data were disclosed during the period beginning twelve months before the date of the service of the enforcement notice concerned and ending immediately before such compliance, of the rectification, erasure or statement concerned, if such compliance materially modifies the data concerned.

(5) The Commissioner may cancel an enforcement notice and, if he or her does so, shall notify in writing the person on whom it was served accordingly.

Failure to comply with enforcement notice an offence

29. (1) A person shall not, without reasonable excuse, fail or refuse to comply with a requirement specified in an enforcement notice.

Section III

(2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine not exceeding twenty five thousand dollars or to imprisonment for a term not exceeding six months or to both such fine and imprisonment.

Investigations in private

30. (1) All investigations of a complaint pursuant to this Act shall be conducted in private.

(2) In the course of an investigation of a complaint under this Act by the Commissioner, the person who made the complaint and the permanent secretary of the public authority or the chief executive officer of any other entity, shall be given an opportunity to make representations to the Commissioner, but no one is entitled as of right to be present during, to have access to, or to comment on, representations made to the Commissioner by any other person.

Referral to Commissioner of Police

31. On completion of an investigation under this Act, the Commissioner shall, where the investigation reveals that an offence has been committed under this Act or the Regulations the Commissioner shall refer the matter to the Commissioner of Police for necessary action.

Register of data controllers

40. The Commissioner shall keep a register to be known as the Register of Data Controllers in which the Commissioner shall cause to be entered in relation to each data controller, the following particulars-
(a) the name and address;
(b) the date of registration;
(c) a description of the personal data processed by or on behalf of the data controller and of the category or categories of personal data subjects to which they relate;
(d) a description of the purpose or purposes for which the personal data is processed;
(e) a description of any recipient or recipients to whom the data controller intends or may wish to disclose the personal data; and
(f) the names, or a description of, any countries or territories outside the Saint Lucia to which the data controller directly or indirectly transfers, or intends or may wish directly or indirectly to transfer, the personal data.

43. Any data controller, who without reasonable excuse processes any personal data without being registered under this Part commits an offence and shall, on summary conviction, be liable to a fine not exceeding twenty five thousand dollars or to imprisonment for a term not exceeding six months or to both.

45. (1) The Commissioner shall keep the Register in the office of the Commissioner and shall at all reasonable times make it available for inspection by any person free of charge.

(2) A person may, on payment of the prescribed fee, obtain from the Commissioner a certified copy of, or of an extract from, an entry in the Register.

St. Vincent and the Grenadines – FAIR – Clear articulation of the power to initiate investigations. However, the enforcement provisions are relatively weak and based on voluntary action on the part of the public authority.

23. (1) Subject to this Act, the Commissioner shall receive and investigate a complaint from any person in respect of any matter relating to -
(a) the collection, retention or disposal of personal information by a public authority; or
(b) the use or disclosure of personal information held by a public authority;

Section III

(2) Nothing in this Act precludes the Commissioner from receiving and investigating complaints of a nature described in subsection (1) that are submitted by a person authorised by the complainant to act on behalf of the complainant, and reference to a complainant in any other section includes a reference to a person so authorised.

(3) Where the Commissioner is satisfied that there are reasonable grounds to investigate a matter under this Act, the Commissioner may initiate a complaint in respect thereof.

24. (1) A complaint under this Act shall be made to the Commissioner in writing unless the Commissioner authorises otherwise.

(2) The Commissioner shall give such reasonable assistance as is necessary in the circumstances to enable any person who wishes to make a complaint to the Commissioner, to put the complaint in writing.

25. Before commencing an investigation of a complaint under this Act, the Commissioner shall notify the chief executive officer of the public authority concerned of the intention to carry out the investigation and shall inform the chief executive officer of the substance of the complaint.

26. Subject to this Act, the Commissioner may determine the procedure to be followed in the discharge of any duty or the performance of any function of the Commissioner under this Act.

27. (1) Every investigation of a complaint under this Act by the Commissioner shall be conducted in private.

(2) In the course of an investigation of a complaint under this Act by the Commissioner, the complainant and the chief executive officer of the public authority concerned shall be given an opportunity to make representations to the Commissioner, but no one is entitled as of right to be present during a hearing or, to have access to, or to comment on, representations made to the Commissioner by any other person.

28. (1) The Commissioner has, in relation to carrying out of the investigation of any complaint under this Act, the power -

(a) to summon and enforce the appearance of persons before the Commissioner and compel them to give oral or written evidence on oath and to produce such documents and things as the Commissioner deems requisite to the full investigation and consideration of the complaint, in the same manner and to the same extent as the High Court;

(b) to administer oaths;

(c) to receive and accept such evidence and other information, whether on oath or by affidavit or otherwise, as the Commissioner sees fit, whether or not the evidence or information is or would be admissible in a court of law;

(d) to enter any premises occupied by any public authority on satisfying any security requirements of the authority relating to the premises;

(e) to converse in private with any person in any premises entered pursuant to paragraph (d) and otherwise carry out therein such inquiries within the power of the Commissioner under this Act as the Commissioner sees fit; and

(f) to examine or obtain copies of or extracts from books or other records found in any premises entered pursuant to paragraph (d) containing any matter relevant to the investigation.

Section III

(2) Notwithstanding any other Act of Parliament or any privilege under the law of evidence, the Commissioner may, during the investigation of any complaint under this Act, examine any information recorded in any form held by a public authority and no information that the Commissioner may examine under this subsection may be withheld from the Commissioner on any grounds.

(3) Any document or things produced pursuant to this section by any person or public authority shall be returned by the Commissioner within a reasonable time after a request is made to the Commissioner by that person or authority, but nothing in this subsection precludes the Commissioner from again requiring its production in accordance with this section.

29. (1) If, on investigating a complaint under this Act in recommendations in respect of personal information, the Commissioner finds that the complaint is well-founded, the Commissioner shall provide to the Minister and the chief executive officer of the public authority that has control of the personal information with a report containing -

(a) the findings of the investigation and any recommendations that the Commissioner considers appropriate; and

(b) where appropriate, a request that, within a time specified therein, notice be given to the Commissioner of any action taken or proposed to be taken to implement the recommendations contained in the report or reasons why no such action has been or is proposed to be taken.

(2) The Commissioner shall, after investigating a complaint under this Act, report to the complainant the results of the investigation, but where a notice has been requested under paragraph (1) (b), no report shall be made under this subsection until the expiration of the time within which the notice is to be given to the Commissioner.

(3) Where a notice has been requested under paragraph (1) (b) but no such notice is received by the Commissioner within the time specified therefore or the action described in the notice is , in the opinion of the Commissioner, inadequate or inappropriate or will not be taken in a reasonable time, the Commissioner shall so advise the complainant in his report under subsection (2) and may include in the report such comments on the matter as he thinks fit.

(4) Where, following the investigation of a complaint, the Commissioner has made recommendations to a public authority under subsection (1), and the decision of the public authority is -

(a) not to implement the recommendations; or

(b) to implement the recommendations, but, in the opinion of the Commissioner, not within a reasonable time or in a manner that is inadequate or inappropriate,

the complainant is entitled to seek judicial review of the decision of the public authority.

30. (1) The Commissioner may, from time to time at the discretion of the Commissioner, carry out an investigation in respect of personal information under the control of a public authority to ensure compliance with sections 7 to 14 of this Act.

(2) Sections 25 to 28 apply, where appropriate and with such modifications as the circumstances require, in respect of investigations carried out under subsection (1).

(3) If, following an investigation under subsection (1), the Commissioner considers that a public authority has not complied with sections 7 to 14 of this Act, the Commissioner shall provide the Minister and the chief executive officer of the authority with a report containing the findings of the investigation and any recommendations that the Commissioner considers appropriate.

(4) Any report made by the Commissioner under subsection (3) may be included in a report made to Parliament pursuant to this Act.

Trinidad and Tobago* – LIMITED (GOOD) – Clear articulation of investigative powers. Clear outline of process by which Commissioner engages both public and private sectors in support of an investigation. The processes, and decisions coming out of same, are backed up by a regime of offences.

58. An individual who has filed a request for his personal information pursuant to section 52 or who has requested correction of personal information pursuant to section 57 may appeal any decision of the head of the public authority to the Commissioner.

59. An appeal to the Commissioner under section 58 shall be made within six weeks of the date when the notice was given of the decision appealed from, by filing with the Commissioner written notice of appeal.

60. The Commissioner may dismiss an appeal if the notice of appeal does not present a reasonable basis for concluding that the personal information to which the notice relates exists.

61. Upon receiving the notice of appeal, the Commissioner shall inform the head of the public authority concerned and any other affected person of the notice of appeal.

62. The Commissioner may authorize a mediator to investigate the circumstances of the appeal and to try to effect a settlement of the matter under appeal.

63. (1) The Commissioner may conduct an enquiry to review the decision of the head of a public authority if the Commissioner has–

(a) not authorized a mediator to conduct an investigation under section 62; or

(b) authorized a mediator to conduct an investigation under section 62, but no settlement has been reached.

(2) Where the Commissioner conducts an enquiry under this section he may on the conclusion of such enquiry either–

(a) affirm the decision of the head of the public authority; or

(b) order the head of the public authority to release the personal information or make the corrections requested.

64. The enquiry by the Commissioner or a mediator and any meetings held by a mediator with parties to the appeal may be conducted in private.

65. The individual who requested access to personal information, the head of the public authority concerned and any affected party shall be given the opportunity to make representations to the Commissioner, but none is entitled to–

(a) be present during;

(b) have access to; or

(c) comment on,

representations made to the Commissioner by any other person.

66. An individual who requests access to personal information, the head of the public authority concerned and any affected party may be represented by counsel or an agent.

67. Where a public authority refuses to give access to personal information, the burden of proof that the information lies within one of the specified exemptions of the Act is on a balance of probabilities and lies upon the public authority.

Section III

76. Where an organization is subject to a mandatory code of conduct and an individual has a reasonable belief that the organization has within its custody or control personal information regarding that individual, the individual may–

(a) where the individual has requested access to or the correction of personal information held by an organization and the organization has refused such request, ask the Commissioner to conduct a review of the resulting decision, act or failure to act of the organization; or

(b) make a complaint to the Commissioner regarding an alleged failure of the organization to comply with the provisions of the mandatory code of conduct.

80. (1) Subject to section 81(2), the Commissioner may conduct an enquiry into a request or complaint under section 76.

(2) Where the Commissioner conducts an enquiry under this section he may, on the conclusion of such enquiry either–

(a) affirm the decision of the organization; or

(b) order the head of an organization to release the personal information requested.

81. (1) The Commissioner may authorize a mediator to investigate the circumstances of the request and to try to effect a settlement of the matter.

(2) Where the Commissioner has–

(a) not authorized a mediator to conduct an investigation under subsection (1); or

(b) authorized a mediator to conduct an investigation under subsection (1) but no settlement has been reached, he may conduct an enquiry into a request under section 80.

82. An enquiry by the Commissioner or a mediator and any meetings held by a mediator with parties to the request may be conducted in private.

83. An individual who requested access to personal information, the head of the organization concerned and any affected party shall be given the opportunity to make representations to the Commissioner, but none is entitled to–

(a) be present during;

(b) have access to; or

(c) comment on,

representations made to the Commissioner by any other person.

84. Every director and officer of a corporation shall take reasonable care to ensure that the corporation complies with–

(a) this Act and the regulations made thereunder; and

(b) any Orders imposed by the Commissioner or his delegate.

93. (1) A person who commits an offence under this Act is liable upon–

(a) summary conviction, to a fine of not more than fifty thousand dollars or to imprisonment for a term of three years; and

(b) conviction on indictment, to a fine of not more than one hundred thousand dollars or to imprisonment for a term of not more than five years.

(2) Where the offence under this Act is committed by a body corporate, the body corporate shall be liable upon–

(a) summary conviction, to a fine of two hundred and fifty thousand dollars; and

(b) conviction on indictment, to a fine of five hundred thousand dollars.

Section III

94. (1) Where a corporation contravenes any of the provisions of this Act, the Court may impose a fine up to ten per cent of the annual turnover of the enterprise.

(2) In imposing a fine under subsection (1) the Court shall take into account–

(a) the estimate of the economic cost of the contravention to the consumers, users of the services in question or any other person affected by the contravention;
(b) the estimate of the economic benefit of the contravention to the enterprise;
(c) the time for which the contravention is in effect if continuing;
(d) the number and seriousness of any other contraventions, if any, committed by the corporation; and
(e) any other matter the Court may consider appropriate in the circumstances.

International Examples and Regional Harmonization

OECD

Accountability Principle

OECD (1980) Principle 8 – A data controller should be accountable for complying with measures which give effect to the principles stated above.

UN

Guidelines Concerning Computerized Personal Data Files (1990)

Field of Application

UN (1990) 10 – The present principles should be made applicable, in the first instance, to all public and private computerized files as well as, by means of optional extension and subject to appropriate adjustments, to manual files. Special provision, also optional, might be made to extend all or part of the principles to files on legal persons particularly when they contain some information on individuals.

European Union

Directive 95/ 46/ EC

Article 28

3. Each authority shall in particular be endowed with:

– investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,
– effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,
– the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.

5. Each supervisory authority shall draw up a report on its activities at regular intervals. The report shall be made public.

6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

7. Member States shall provide that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard.

3.2.4 Collection of Personal Information

International Best Practices and Regional Trends:

- The framework provides for the notification of the data subject of the purpose for the collection of personal information.
- The framework limits the type of data collected for a given purpose.
- The framework provides for the data subjects assent of data collection.
- The framework recognizes the particular demands for information protection in the health sector with regard to data collection.

Regional Examples

Antigua and Barbuda – NONE

Bahamas – GOOD – Clear articulation of principles in adherence to Data Protection principles.

6.(1) A data controller shall comply with the following provisions in relation to personal data kept by him -

(a) the data or the information constituting the data shall have been collected by means which are both lawful and fair in the circumstances of the case;

(b) the data is accurate and, where necessary, kept up to date, (except in the case of back-up data);

(c) the data -

(i) shall be kept only for one or more specified and lawful purposes,

(ii) shall not be used or disclosed in any manner incompatible with that purpose or those purposes,

(iii) shall be adequate, relevant and not excessive in relation to that purpose or those purposes, and

(iv) shall not be kept for longer than is necessary for that purpose or those purposes, except in the case of personal data kept for historical, statistical or research purposes; and

(d) appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction.

(2) In determining for the purposes of subsection (1)(a) of this section, whether personal data or information constituting such data are fair in the circumstances of the case, regard is to be had to the method by which they are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be processed:

Provided however that the data or the information constituting such data shall not be regarded for the purposes of subsection (1)(a) of this section as having been obtained unfairly by reason only that its use for any such purpose was not' disclosed when it was obtained, if the data are not used in such a way that damage or distress is, or is likely to be, caused to any data subject.

(3) A data processor shall, as respects personal data processed by him, comply with subsection (1)(d) of this section.

7. Subsection (1)(a) of section 6 shall not apply to information intended for inclusion in data, or to data, kept for a purpose mentioned in paragraph (a) of section 9, in any case in which the application of that paragraph to the data would be likely to prejudice any of the matters mentioned in paragraph (a) of section 9.

…

20. (1) The Commissioner may encourage trade associations and other bodies representing categories of data controllers to prepare codes of practice to be complied with by those categories in dealing with personal data.

(2) The Commissioner may approve of any code of practice so prepared (referred to subsequently in this section as a code) if he is of opinion that it provides for the data subjects concerned protection with regard to personal data relating to them that conforms with that provided for by sections 6, 8 (other than subsection (9)) and 10 and shall encourage its dissemination to the data controllers concerned.

(3) Any such code that is approved by the Commissioner shall be laid by the Minister before each House of Parliament and shall be subject to affirmative resolution of each House.

(4) In subsection (3), “affirmative resolution of each House” means that such code shall not come into operation unless and until affirmed by a resolution of each House of Parliament.

(5) This section shall apply in relation to data processors as it applies in relation to categories of data controllers with the modification that the references in this section to the said sections shall be construed as references to subsection (1)(d) of section 6 and with any other necessary modifications.

Barbados – NONE

Belize – NONE

Dominican Republic – NONE

Dominica, Grenada – NONE

Jamaica – NONE

St. Kitts and Nevis – LIMITED – Draft legislation is reported to be in preparation before presentation to Parliament, and is as such confidential. Copies of the draft were not available for assessment.

St. Lucia* – LIMITED (GOOD) – Clear articulation of principles in adherence to Data Protection principles.

Collection of personal data

32. (1) Subject to Part 6, a data controller shall not collect personal data unless –
- (a) it is collected for a lawful purpose connected with a function or activity of the data controller; and
- (b) the collection of the data is necessary for that purpose;

(2) Where a data controller collects personal data directly from a data subject, the data controller shall at the time of collecting personal data ensure that the data subject concerned is informed of –
- (a) the fact that the personal data is being collected;
- (b) the purpose for which the personal data is being collected;
- (c) the intended recipients of the personal data;
- (d) the name and address of the data controller;
- (e) whether or not the supply of the personal data by that data subject is voluntary or mandatory;
- (f) the consequences for that data subject if all or any part of the requested personal data is not provided;
- (g) whether or not the personal data collected will be further processed and whether or not the consent of the data subject will be required for the further processing; and
- (h) the data subject's right of access to, the possibility of correction of and destruction of, the personal data to be provided.

(3) A data controller shall not be required to comply with subsection (2) –
- (a) in respect of a data subject where –
  - (i) compliance with subsection (2) in respect of a second or subsequent collection will be to repeat, without any material difference, what was done to comply with that subsection in respect of the first collection; and
  - (ii) not more than twelve months have elapsed between the first collection and this second or subsequent collection; or
- (b) where –
  - (i) compliance is not reasonably practicable at the time of collection, provided that the data controller makes available to the data subject all the relevant information specified in subsection (2) as soon as practicable; or
  - (ii) the personal data is used in a form in which the data subject concerned cannot or could not reasonably expect to be identified.

Section III

(4) Where personal data is not collected directly from the data subject concerned, the data controller or any person acting on his behalf shall ensure that the data subject is informed of the matters specified in subsection (2).

(5) Subsection (3) shall not operate to prevent a second or subsequent collection from becoming a first collection where the data controller has complied with subsection (2) in respect of the second or subsequent collection.

(6) A data controller who contravenes this section commits an offence and is liable to a fine not exceeding twenty five thousand dollars or to imprisonment for a term not exceeding six months.

…

St. Vincent and the Grenadines – GOOD – Clear articulation of principles in adherence to Data Protection principles. Includes good language including exemptions with regard to National Security, Pubic Health concerns etc.

7. (1) A public authority shall not collect personal information unless -
   (a) the information is collected for a lawful purpose directly related to a function or activity of the authority; and
   (b) the collection of the information is necessary for, or directly related to, that purpose.

(2) A public authority shall not collect personal information -
   (a) by unlawful means; or
   (b) by means that, in the circumstances of the case -
      (i) are unfair; or
      (ii) intrude to an unreasonable extent upon the personal affairs of the individual concerned.

8. (1) A public authority may, subject to subsection (3), collect personal information directly from the individual concerned.

(2) At or before the time, or if that is not practicable, as soon as practicable after, a public authority collects personal information under subsection (1), the authority shall take such steps as are, in the circumstances, reasonable to ensure that the individual concerned is aware of -
   (a) the purposes for which the information is being collected;
   (b) the fact that the collection of the information is authorised or required by or under law, if such collection is so authorised or required; and
   (c) the intended recipients of the information.

(3) A public authority is not obliged to comply with subsection (1) where -
   (a) the information is publicly available information;
   (b) the individual concerned authorises the collection of the information from someone else;
   (c) non-compliance will not prejudice the interests of the individual concerned;
   (d) non-compliance is necessary -
      (i) for the prevention, detection, investigation, prosecution or punishment of any offence or breach of law;
      (ii) for the enforcement of a law imposing a pecuniary or custodial penalty or both;
      (iii) for the protection of public revenue;
      (iv) for the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal;
      (v) in the interests of national security; or
      (vi) for the prevention of the spread of a communicable or contagious disease;

Section III

(e) compliance would prejudice the purpose of the collection; or
(f) compliance is not reasonably practicable in the circumstances of the particular case.

11. (1) Subject to section 12, where a public authority holds personal information, it shall not disclose the information to a person, body or agency (other than the individual concerned), unless -
(a) the individual concerned has expressly or impliedly consented to the disclosure;
(b) the disclosure of the information is required or authorised by or under law;
(c) the disclosure of the information is one of the purposes in connection with which the information was collected, or is directly connected to that purpose;
(d) the individual concerned is reasonably likely to have been aware or made aware under section 8 (2) (c) that information of that kind is usually passed on to that person, body or agency;
(e) the information is to be disclosed -
(i) in a form in which the individual concerned is not identified; or
(ii) for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or
(f) the authority believes on reasonable grounds that disclosure of the information is necessary -
(i) to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or other person, or to public health or safety;
(ii) for the prevention, detection, investigation, prosecution or punishment of any offence or breach of law;
(iii) the enforcement of a law imposing a pecuniary or custodial penalty or both;
(iv) the protection of public revenue;
(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal; or
(vi) in the interests of national security.

(2) Any person, body or agency to whom personal information is disclosed under subsection (1) shall not use or disclose the information for a purpose other than the purpose for which the information was given to that person, body or agency.

12. A public authority shall only use or disclose personal information under section 10 or section 11, where such use or disclosure would not amount to an unreasonable invasion of privacy of the individual concerned, taking into account the specific nature of the personal information and the specific purpose for which it is to be so used or disclosed.

13. Where a public authority holds personal information, it shall ensure that -
(a) the information is protected, by such security safeguards as is reasonable in the circumstances to take, against loss, unauthorised access, use, modification or disclosure, and against other misuse; and
(b) where it is necessary for the information to be given to a person, body or agency in connection with the provisions of a service to the authority, everything reasonably within the power of the authority is done to prevent unauthorised use or disclosure of the information.

Trinidad and Tobago* – LIMITED (GOOD) – Clear articulation of principles in adherence to Data Protection principles

30. Personal information may not be collected by or for a public authority unless–
(a) the collection of that information is expressly authorized by or under any written law;
(b) the information is collected for the purposes of law enforcement; or
(c) that information relates directly to and is necessary for an operating programme or activity of the public authority.

Section III

31. (1) Where a public authority requires personal information from an individual it shall collect the personal information or cause the personal information to be collected directly from that individual.

(2) Notwithstanding subsection (1), personal information may be collected from a source other than the individual where–

(a) another method of collection is authorized by the individual, by the Commissioner or by any other written law;

(b) the collection of information is necessary for medical treatment of an individual and it is not possible to collect the information directly from that individual or the collection is necessary to obtain authority from that person for another method of collection; and

(c) the information is collected for the purpose of–

(i) determining the suitability for an honour or award including an honorary degree, scholarship, prize or bursary;

(ii) proceedings before a court or a judicial or *quasi*-judicial tribunal;

(iii) collecting a debt or fine or making a payment; or

(iv) law enforcement.

32. (1) A public authority shall ensure that the individual from whom it collects personal information or causes personal information to be collected is informed of–

(a) the purpose for collecting it;

(b) the legal authority for collecting it; and

(c) the title, business address and business telephone number of an official or employee or the public authority who can answer the individual's questions about the collection.

(2) Subsection (1) shall not apply if compliance with subsection (1) would–

(a) result in the collection of inaccurate information;

(b) defeat the purpose or prejudice the use for which the information is to be collected;

(c) prejudice a law enforcement matter; or

(d) prejudice the defence of Trinidad and Tobago or of any foreign state allied to or associated with Trinidad and Tobago or harm the detection, prevention or suppression of espionage, sabotage or terrorism.

33. Personal information that has been used by a public authority for an administrative purpose shall be retained by the authority for such period of time after it has been used as may be prescribed by Order of the Minister, to ensure that the individual to whom it relates has a reasonable opportunity to obtain access to that information.

34. Where the personal information of an individual is in the custody or control of a public authority and the personal information will be used by or on behalf of the public authority to make a decision that directly affects the individual, the public authority shall make every reasonable effort to ensure that the personal information is accurate and complete.

…

68. A person who–

(a) collects, retains, manages, uses, processes or stores personal information in Trinidad and Tobago;

(b) collects personal information from individuals in Trinidad and Tobago; or

(c) uses an intermediary or telecommunications service provider located in Trinidad and Tobago to provide a service in furtherance of paragraph *(a)* or *(b)*,

shall follow the General Privacy Principles set out in section 6 in dealing with personal information.

Section III

69. The Commissioner shall consult with industry to promote the application of the General Privacy Principles through the development of codes of practice through such means as–

(a) providing guidance on the development of codes of practice;
(b) providing guidance on compliant resolution mechanisms;
(c) fostering education on the General Privacy Principles;
(d) working with government and private sector bodies to promote awareness of codes of conduct among consumers; and
(e) taking any action that appears to the Commissioner to be appropriate.

70. (1) Notwithstanding section 68 where, in the opinion of the Commissioner, the public interest warrants the immediate and mandatory development of codes of conduct dealing with the application of the General Privacy Principles to a particular industry, economic sector, or activity, the Commissioner may, by Order, require the development of a code of conduct and set a time limit for its development.

(2) Subject to subsection (1) where there is an appropriate government regulator of an industry, economic sector or activity, the Commissioner may request the regulator to oversee the development of the code of conduct for that industry, economic sector or activity

International Examples and Regional Harmonization

OECD

Collection Limitation Principle

OECD (1980) Principle 1 – There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Purpose Specification Principle

OECD (1980) Principle 3 – The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

United Nations

Guidelines Concerning Computerized Personal Data Files (1990)

UN (1990) Principle 3 – The purpose which a file is to serve and its utilization in terms of that purpose should be specified, legitimate and, when it is established, receive a certain amount of publicity or be brought to the attention of the person concerned, in order to make it possible subsequently to ensure that:

(a) All the personal data collected and recorded remain relevant and adequate to the purposes so specified;
(b) None of the said personal data is used or disclosed, except with the consent of the person concerned, for purposes incompatible with those specified;
(c) The period for which the personal data are kept does not exceed that which would enable the achievement of the purposes so specified.

European Union

Directive 95/ 46/ EC

Article 7

Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
(d) processing is necessary in order to protect the vital interests of the data subject; or
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

3.2.5 Use of personal information

International Best Practices and Regional Trends:

- The framework limits the collecting party's use of information collected to that which was notified to, and assented by, the data subject.
- The framework limits the collecting party's retention of information to that period for which it is necessary.
- The framework obliges the collecting agency to ensure correctness of information.
- The framework obliges the collecting agency to safeguard the information collected.
- The framework provides for the subject's validation of the information stored.
- The framework provides for the oversight body approving particular types of information processing.

Regional Examples

Antigua and Barbuda – NONE

Bahamas – GOOD – While there is substantial provision for the limitation of collection and use of information and for individual participation of the data subject, but there seems insufficient provision for the Data Commissioner's oversight of types of information processing.

6.(1) A data controller shall comply with the following provisions in relation to personal data kept by him -

Section III

(e) the data -
  (i) shall be kept only for one or more specified and lawful purposes,
  (ii) shall not be used or disclosed in any manner incompatible with that purpose or those purposes,
  (iii) shall be adequate, relevant and not excessive in relation to that purpose or those purposes, and
  (iv) shall not be kept for longer than is necessary for that purpose or those purposes, except in the case of personal data kept for historical, statistical or research purposes; and

(f) appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction.

8.(1) Subject to the provisions of this Act, any individual who makes a written request to a data controller has a right, within forty days after complying with the provisions of this section, to -

(a) be informed by the data controller whether the data kept by him include personal data relating to the individual;

(b) be supplied by the data controller with a copy of the information constituting any such data; and

(c) where any of the information is expressed in terms that are not intelligible to the average person without explanation, the information shall be accompanied by an explanation of those terms.

(2) A request for the information specified in subsection (1)(a) shall, in the absence of any indication to the contrary, be treated as including a request for a copy of the information specified in subsection (1)(b).

(3) The Minister may by regulations prescribe the fee to be charged by a data controller in respect of such a request as aforesaid, and any fee so paid shall be reimbursed where the request is not complied with or the data controller rectifies, supplements, or erases part of, the data concerned (and thereby materially modifies the data) or erases all of the data on the application of the individual or in accordance with an enforcement notice hereunder or court order.

(4) An individual making a request under this section shall supply the data controller concerned with such information as he may reasonably require in order to satisfy himself of the identity of the individual and to locate any relevant personal data or information.

(5) Nothing in subsection (1) obliges a data controller to disclose to a data subject personal data relating to another individual unless that other individual has consented to the disclosure:

Provided that, where the circumstances are such that it would be reasonable for the data controller to conclude that, if any particulars identifying that other individual were omitted, the data could then be disclosed as aforesaid without his being thereby identified to the data subject, the data controller shall be obliged to disclose the data to the data subject with the omission of those particulars.

(6) Information supplied pursuant to a request under subsection (1) may take account of any amendment of the personal data concerned made since the receipt of the request by the data controller (being an amendment that would have been made irrespective of the receipt of the request) but not of any other amendment.

(7) A notification of a refusal of a request made by an individual under the preceding provisions of this section shall be in writing and shall include a statement of the reasons for the refusal and an indication that the individual may complain to the Commissioner about the refusal.

Section III

(8) Where a data controller has previously complied with a request made under subsection (1) by an individual, the data controller is not obliged to comply with a subsequent, identical or similar request under that subsection by that individual unless a reasonable interval has elapsed between compliance with the previous request and the making of the current request.

(9) In determining for the purposes of subsection (8) whether requests under subsection (1) are made at reasonable intervals, regard shall be had to the nature of the data, the purposes for which the data are processed and the frequency with which the data are altered.

9. Section 8 shall not apply to personal data -

(a) kept for the purpose of preventing, detecting or investigating an offence or a breach of agreement, apprehending or prosecuting offenders or assessing or collecting any tax, duty or other moneys owed or payable to the Government, a local authority, a statutory corporation, or a public body, in any case in which the application of that section to the data would be likely to prejudice any of the matters aforesaid;

(b) to which, by virtue of paragraph (a) section 8 does not apply and which are kept for the purpose of discharging a function conferred by or under any enactment and consisting of information obtained for such a purpose from a person who had it in his possession for any of the purposes mentioned in paragraph (a);

(c) in any case in which the application of section 8 would be likely to prejudice the security of, or the maintenance of good order and discipline in a prison, a place of detention provided under the Prisons Act, or any other enactment under the laws of The Bahamas;

(d) kept for the purpose of performing such functions conferred by or under any enactment as may be specified by regulations made by the Minister, being functions that, in the opinion of the Minister, are designed to protect members of the public against financial loss in any case in which the application of that section to the data would be likely to prejudice the proper performance of any of those functions, occasioned by -

(i) dishonesty, incompetence or malpractice on the part of persons concerned in the provision of banking, insurance, investment or other financial services or in the management of companies or similar organisations, or

(ii) the conduct of persons who have at any time been adjudicated bankrupt;

(e) in respect of which the application of that section would be contrary to the interests of protecting the international relations of The Bahamas;

(f) consisting of an estimate of, or kept for the purpose of estimating, the amount of the liability of the data controller concerned based on a claim for the payment of a sum of money, whether in respect of damages or compensation, in any case in which the application of section 8 would be likely to prejudice the interests of the data controller in relation to the claim;

(g) in respect of which a claim of privilege could be maintained in proceedings in a court in relation to communications between a client and his. professional legal advisers or between those advisers;

(h) kept only for the purpose of preparing statistics or carrying out research if the data are not used or disclosed (other than to a person to whom a disclosure of such data may be made in the circumstances specified in section 13) for any other purpose and the resulting statistics or the results of the research are not made available in a form that identifies any of the data subjects;

(i) in any case in which the application of that section would reveal confidential commercial information which cannot be severed from the record containing the personal information for which access is requested; or

(j) that are back-up data.

Section III

10.(1) An individual shall, upon submission of a written request to a data controller who keeps personal data relating to him, be entitled to have rectified or, where appropriate, erased any such data in relation to which there has been a contravention of subsection (1) of section 6 by the data controller and the data controller shall comply with the request within forty days after it has been given or sent to him:

Provided that the data controller shall, as respects data that are inaccurate or not kept up to date, be deemed -

(a) to have complied with the request if he supplements the data with a statement (to the terms of which the individual has agreed) relating to the matters dealt with by the data; and

(b) if he supplements the data as aforesaid, not to be in contravention of subsection (1) (b) of section 6.

(2) In complying with a request under subsection (1) of this section, a data controller shall, within forty days after the request has been given or sent to him, notify the individual making the request of such compliance.

11. Where a data subject makes a written request for the data controller to cease using, for the purpose of direct marketing, any data which was kept for that purpose, the data controller shall, as soon as may be and in any event not more than forty days after the request has been given or sent to him -

(i) erase all data as was kept for the purpose aforesaid, or

(ii) if the data are kept for that purpose and other purposes, cease using the data for that purpose, and

(iii) notify the data subject in writing accordingly.

Barbados – NONE

Belize – NONE

Dominican Republic – NONE

Dominica, Grenada – NONE

Jamaica – NONE

St. Kitts and Nevis – LIMITED – Draft legislation is reported to be in preparation before presentation to Parliament, and is as such confidential. Copies of the draft were not available for assessment.

St. Lucia* – LIMITED (GOOD) – While there is substantial provision for the limitation of collection and use of information and for individual participation of the data subject, but there seems insufficient provision for the Data Commissioner's oversight of types of information processing.

33. (1) Subject to subsections (2), (3) and (4), a data controller shall not process personal data unless the data controller has obtained the express consent of the data subject.

(2) A data controller may process personal data without obtaining the express consent of the data subject where the data subject has published the personal data.

(3) A data controller may process personal data, without obtaining the express consent of the data subject, for health and hospital care purposes, provided that the personal data is processed by a health care professional subject to the obligation for professional secrecy or professional confidentiality and the processing is necessary for-

(a) preventative medicine and the protection of public health;

(b) medical diagnosis;

Section III

(c) health care or treatment; or
(d) management of health and hospital care services.

(4) A data controller may process personal data without obtaining the express consent of the data subject where the processing is necessary –
(a) for the performance of a contract to which the data subject is a party;
(b) in order to take steps required by the data subject prior to entering into a contract;
(c) in order to protect the vital interests of the data subject or another person, in a case where-
(i) consent cannot be physically or legally be given by or on behalf of the data subject or a given; or
(ii) the data controller cannot reasonably be expected to obtain the consent of the data subject ;
(d) for compliance with any legal obligation to which the data controller is subject;
(e) for the administration of justice;
(f) for the performance of an activity that is carried out in the public interest or in the exercise of official authority vested in the data controller or in a third party to whom the personal data is disclosed; or
(g) for a purpose that concerns a legitimate interest of the data controller or of such a third party to whom personal data is provided, except where such interest is overridden by the interest to protect the fundamental rights and freedoms of the data subject and in particular the right to privacy;

(4) Where the processing of personal data is done pursuant to paragraphs (f) and (g) of subsection (4), the data subject, except where otherwise provided in any other law, shall be entitled to object at any time to the data controller on compelling legitimate grounds to the processing of the personal data.

(5) Where the processing of personal data takes place with the consent of the data subject, the data subject may at any time revoke his or her consent for compelling legitimate grounds relating to his particular situation.

(6) A data controller who contravenes this section commits an offence and is liable to a fine not exceeding twenty five thousand dollars or to imprisonment for a term not exceeding six months.

(7) For the purposes of this section "health care professional" has the meaning given to it pursuant to the [Health Practitioners Act 2006, No. 33]

34. (1) A data controller shall take all reasonable steps to ensure that personal data within the data controller's possession is –
(a) accurate; and
(b) kept up to date where such data requires regular updating.

(2) A data controller who contravenes this section commits an offence and is liable to a fine not exceeding twenty five thousand dollars or to imprisonment for a term not exceeding six months.

35. (1) The data controller shall ensure that personal data is –
(a) kept only for one or more specified and lawful purposes for which the personal data has been collected and processed;
(b) not used or disclosed in any manner incompatible with the purposes for which the personal data has been collected and processed;
(c) adequate, relevant and not excessive in relation to the purposes for which the personal data has been collected and processed; and

Section III

(d) not kept for longer than is necessary for the purposes for which the personal data has been collected and processed.

(2) A data controller who contravenes this section commits an offence and is liable to a fine not exceeding twenty five thousand dollars or to imprisonment for a term not exceeding six months.

36.(1) A data controller shall –

(a) take appropriate security and organizational measures for the prevention of unauthorized access to, alteration of, disclosure of, accidental loss, and destruction of the personal data in the data controller's control; and

(b) ensure that the measures provide a level of security appropriate to –

(i) the harm that is likely to result from the unauthorized access to, alteration of, disclosure of, destruction of the data and its accidental loss; and

(ii) the nature of the data concerned.

(2) A data controller shall take all reasonable steps to ensure that any person employed by the data controller is aware of and complies with the relevant security measures.

(3) Without prejudice to subsection (1), in determining the appropriate security measures, in particular, where the processing involves the transmission of personal data over an information and communication network, a data controller shall have regard to –

(a) the state of technological development available;

(b) the cost of implementing any of the security measures;

(c) the special risks that exist in the processing of the personal data; and

(d) the nature of the personal data being processed.

(4) A data controller who contravenes this section commits an offence and is liable to a fine not exceeding twenty five thousand dollars or to imprisonment for a term not exceeding six months.

37. (1) Where personal data is no longer required for the purpose for which it was collected, the data controller shall forthwith destroy the personal data and render it inaccessible electronically-

(a) destroy the personal data as soon as reasonably practicable; and

(b) notify any data processor holding the personal data.

(2) A data controller who contravenes this section commits an offence and is liable to a fine not exceeding twenty five thousand dollars or to imprisonment for a term not exceeding six months.

…

46. (1) Subject to section 46, a data controller shall on the written request of a data subject –

(a) provide a written response to the data subject setting out the following-

(i) whether the data kept by the data controller includes personal data relating to the data subject and a description of that personal data, if any;

(ii) the purposes for which the personal data is being or is to be processed;

(iii) the source from which the information is being collected;

(iv) the logic that is involved in any automatic processing of personal data concerning the data subject;

(v) the recipients or classes of recipients to whom they are or may be disclosed; and

(b) permit the data subject to examine the personal data in accordance with the Regulations or supply the data subject or the relevant person with a copy of any personal data referred to in paragraph (a) on payment of the prescribed fee.

Section III

(2) A request under subsection (1) (a) and (b) shall be treated as a single request.

(3) Where access to personal data is given under this Act and the data subject has a sensory disability and requests that access be given in an alternative format, access shall be given in an alternative format if-

(a) the personal data already exists in an alternative format that is acceptable to the data subject; or

(b) the data controller considers it to be reasonable to cause the personal information to be converted.

(3) Where any personal data referred to under subsection (1) is expressed in terms that are not intelligible without explanation, the data controller shall supply the personal data with an explanation of those terms.

(4) A fee paid by a person to a data controller under this section shall be returned to the person where a request under subsection (1) is not complied with.

(5) The information to be supplied pursuant to a request under this section shall be supplied by reference to any personal data at the time when the request is received, except that it may take account of any amendment or deletion made between that time and the time when the information is supplied.

47. (1) Subject to subsection (2) and section 48 and to the payment of the prescribed fee, a data controller shall comply with a request under section 46 not later than thirty days after the receipt of the request.

(2) Where a data controller is unable to comply with the request within the period specified in subsection (1), the data controller shall –

(a) before the expiry of the specified period –

(i) inform the data subject that the data controller is unable to comply with the request and shall, if required, state the reasons for inability to comply;

(ii) seek consent of the data subject for an extension of time for compliance by the data controller; or

(iii) apply to the Commissioner forthwith for an extension of time for compliance by the data controller.

48.(1) A data controller may refuse a request under section 46 where –

(a) the data controller is not supplied with such information as the data controller may reasonably require in order to satisfy himself or herself as to the identity of the person making the request, and to locate the information which the person seeks;

(b) compliance with such request will be in contravention with his confidentiality obligation imposed under this Act or any other enactment.

(2) Where a data controller cannot comply with a request under section 47 without disclosing personal data relating to another person, the data controller may refuse the request unless –

(a) the other individual has consented to the disclosure of his or her personal data to the person making the request; or

(b) the data controller obtains the written approval of the Commissioner.

(3) In determining for the purposes of subsection (2) (b) whether it is reasonable for the Commissioner to approve a request without the consent of the other individual concerned, regard shall be had, in particular, to –

(a) any duty of confidentiality owed to the other individual;

Section III

(b) any steps taken by the data controller with a view to seeking the consent of the other individual;
(c) whether the other individual is capable of giving consent; and
(d) any express refusal of consent by the other individual.

(5) A data controller shall not comply with a request under section 46 where –
(a) he is being requested to disclose information given or to be given in confidence for the purposes of –
(i) the education, training or employment, or prospective education, training or employment, of the data subject;
(ii) the appointment, or prospective appointment, of the data subject to any office; or
(iii) the provision, or prospective provision, by the data subject of any service;
(b) the personal data requested consists of information recorded by candidates during an academic, professional or other examination;
(c) such compliance would, by revealing evidence of the commission of any offence other than an offence under this Act, expose him to proceedings for that offence.

(6) A notification by the data controller of a refusal of a request made by a data subject shall be in writing and shall include a statement of the reasons for the refusal and an indication that the data subject may complain to the Commissioner about the refusal.

49. (1) Where personal data processed by a data controller to which access has been given under any enactment, contains personal data of a data subject which the data subject claims-
(a) is incomplete, incorrect, misleading, or excessive;
(b) not relevant to the purpose for which the document is held;

the data controller shall, upon application of the data subject, cause such data to be rectified, blocked, erased, destroyed, rendered inaccessible or annotated as appropriate.

(2) Where a data controller is aware that a third party holds personal data which is in terms of subsection (1) (a) and (b), he or she shall, as soon as reasonably practicable, require the third party to rectify, block, erase, destroy, render inaccessible or annotate the data, as appropriate.

(3) Where a data controller or a third party fails to rectify, block, erase or destroy personal data in terms of subsection (1) (a) and (b), a data subject may apply to the Commissioner to have such data rectified, blocked, erased, destroyed, rendered inaccessible or annotated as appropriate.

(4) Upon being satisfied by an application under subsection (3) that the personal data is in terms of subsection (1) (a) and (b), the Commissioner shall, where he or she is satisfied, direct the data controller to rectify, block, erase, destroy or annotate those data and any other personal data in respect of which he is the data controller.

(5) Where the Commissioner –
(a) issues a direction under subsection (4); or
(b) is satisfied on the application by an individual that personal data of which the individual is the data subject were inaccurate and have been rectified, blocked, erased, destroyed or annotated,

the Commissioner may direct the data controller to notify third parties to whom the data have been disclosed, of the rectification, blocking, erasure, destruction or annotation.

51. (1) A person may, at any time, by notice in writing revoke consent to the processing of personal data in respect of which he is a data subject.

Section III

(2) Where the data controller receives a notice under subsection (1), the data controller shall, as soon as reasonably practicable, and in any event not more than thirty days after the request is received, stop processing the personal data and delete the personal data and render it inaccessible.

(3) The data controller shall forthwith, in writing, notify the data subject in writing of any action taken under subsections (2).

(4) A data controller who contravenes this section commits an offence and is liable to a fine not exceeding twenty five thousand dollars or to imprisonment for a term not exceeding six months.

St. Vincent and the Grenadines – GOOD – There is substantial provision for the limitation of collection and use of information and for individual participation of the data subject.

9. Where a public authority holds personal information, having regard to the purpose for which the information is proposed to be used, it shall not use that information without taking such steps as are, in the circumstances, reasonable to ensure that, the information is complete, accurate, up to date, relevant and not misleading.

10. Subject to section 12, where a public authority holds personal information that was collected in connection with a particular purpose, it shall not use that information for any other purpose unless -
- (a) the individual concerned authorises the use of the information for that other purpose;
- (b) use of the information for that other purpose is authorised or required by or under law;
- (c) the purpose for which the information is used is directly related to the purpose for which the information was collected;
- (d) the information is used -
  - (i) in a form in which the individual concerned is not identified; or
  - (ii) for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned;
- (e) the authority believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or other person, or to public health or safety; or
- (f) use of information for that other purpose is necessary -
  - (i) for the prevention, detection, investigation, prosecution or punishment of any offence or breach of law;
  - (ii) for the enforcement of a law imposing a pecuniary or custodial penalty or both ;
  - (iii) for the protection of public revenue;
  - (iv) for the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal; or
  - (v) in the interests of national security.

…

13. Where a public authority holds personal information, it shall ensure that -
- (a) the information is protected, by such security safeguards as is reasonable in the circumstances to take, against loss, unauthorised access, use, modification or disclosure, and against other misuse; and
- (b) where it is necessary for the information to be given to a person, body or agency in connection with the provisions of a service to the authority, everything reasonably within the power of the authority is done to prevent unauthorised use or disclosure of the information.

Section III

14. (1) Where a public authority uses personal information for an administrative purpose, it shall retain the information only for such period of time after it is so used as may be prescribed by regulation in order to ensure that the individual concerned has a reasonable opportunity to obtain access to the information, if necessary.

(2) Subject to subsection (1) and this Act, the Minister shall prescribe by regulation, guidelines for the retention and disposal of personal information held by a public authority.

15. (1) Where a document of a public authority to which access has been given under any enactment, contains personal information of a person and that person claims that the information -

(a) is incomplete, incorrect or misleading; or
(b) not relevant to the purpose for which the document is held,

the public authority may, subject to subsection (2), on the application of that person, amend the information upon being satisfied of the claim.

(2) An application under subsection (1) shall -

(a) be in writing; and
(b) as far as practicable, specify:
  (i) the document or official document containing the record of personal information that is claimed to require amendment,
  (ii) the information that is claimed to be incomplete, incorrect or misleading,
  (iii) whether the information is claimed to be incomplete, incorrect or misleading,
  (iv) the applicant's reasons for so claiming, and
  (v) the amendment requested by the applicant.

(3) To the extent that it is practicable to do so, the public authority shall, when making any amendment under this section to personal information in a document, ensure that it does not obliterate the text of the document as it existed prior to the amendment.

(4) Where a public authority is not satisfied with the reasons for an application under subsection (1), it may refuse to make any amendment to the information and inform the applicant of its refusal together with its reasons for so doing.

(5) A person aggrieved by a decision of a public authority to refuse an application for an amendment to information may make a complaint in writing to the Commissioner within twenty-eight days of the date of receipt of the communication of the refusal.

Trinidad and Tobago* – LIMITED (GOOD) – There is substantial provision for the limitation of collection and use of information and for individual participation of the data subject,

35. A public authority shall protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, alteration, disclosure or disposal.

36. A public authority shall ensure or take steps to ensure that personal information in its custody or under its control is stored only in Trinidad and Tobago and accessed only in Trinidad and Tobago unless–

(a) the individual to whom the information relates has identified the information and has consented in the prescribed manner to its being stored in or accessed from another jurisdiction; or
(b) the information is stored in or accessed from another jurisdiction that has comparable safeguards as provided by this Act.

Section III

37. A public authority shall dispose of all personal information in its control or custody in accordance with Regulations made by the Minister under this Act.

38. Personal information under the custody or control of a public authority shall not, without the consent of the individual to whom it relates, be used by the authority except for the purpose for which the information was obtained or compiled by the public authority, or for a use consistent with that purpose, or for a purpose for which the information may be disclosed by the public authority pursuant to section 42.

39. The use of personal information is consistent with the purposes for which it was obtained or compiled, if the use has a reasonable and direct connection to the purpose, and is necessary for performing the statutory duties of, or for operating a legally authorized programme of a public authority that uses or discloses the information or causes the information to be used or disclosed.

40. (1) A public authority shall not process sensitive personal information unless it obtains the consent of the person to whom that sensitive personal information relates.

(2) Notwithstanding subsection (1), sensitive personal information may be processed–

(a) by a health care professional for the purposes of health and hospital care where it is necessary for–

(i) preventative medicine and the protection of public health;
(ii) medical diagnosis;
(iii) health care and treatment; and
(iv) the management of health and hospital care services;

(b) where it has been made public, by the person to whom such information relates;
(c) for research and statistical purposes in accordance with section 43;
(d) in the interest of national security; or
(e) for the purposes of determining access to social services.

(3) For the purpose of this section "health care professional" means a person registered under the–

(a) Medical Board Act;
(b) Dental Profession Act;
(c) Opticians Registration Act;
(d) Pharmacy Board Act; and
(e) Professions Related to Medicine Act.

(4) A person who contravenes this section commits an offence.

…

52. (1) Subject to section 53 every individual who is a citizen of or resident in Trinidad and Tobago has a right to and shall on request, be given access to–

(a) personal information about that individual contained in a personal information bank in the custody and control of a public authority;
(b) any other personal information about the individual under the custody or control of a public authority with respect to which the individual is able to provide sufficiently specific information on the location of the information as to render it reasonably retrievable by the public authority.

(2) A request for access to personal information shall be made to the public authority that has control of the personal information bank or of the information, as the case may be, in the form approved by the Commissioner.

Section III

(3) The head of a public authority may, where reasonable and in appropriate circumstances, provide personal information in accordance with the provisions of this Act in response to an oral request.

(4) For the purpose of this section, "resident" has the meaning assigned to it by the Immigration Act.

53. (1) A head of a public authority may refuse to disclose personal information to the individual to whom the information relates where–

(a) the disclosure would constitute an unjustified invasion of another individual's personal privacy;

(b) it is a correctional record where the disclosure could reasonably be expected to reveal information supplied in confidence;

(c) it is evaluative or opinion material compiled solely for the purpose of determining suitability, eligibility or qualifications for employment or for the awarding of government contracts and other benefits where the disclosure would reveal the identity of a source who furnished information to the institution in circumstances where it may reasonably be assumed that the identity of the source would be held in confidence; and

(d) a disclosure would result in disclosure of information that is exempt from disclosure under Part IV of the Freedom of Information Act.

(2) The head of a public authority may disregard requests from an individual for access to that individual's personal information where it would unreasonably interfere with the operations of the public authority because of the repetitious or systematic nature of the requests or the requests are frivolous or vexatious.

54. (1) A head of a public authority shall make every effort to sever information that is exempt from disclosure pursuant to section 53 from information that may be made available to the individual requesting access to his personal information and make the non-exempt information available.

(2) Where acknowledgment of the existence of information that is exempt from disclosure would reveal critical information about the nature of contents of the information, the head of the public authority may refuse to disclose the existence of the information.

…

74. (1) A corporation shall not process sensitive personal information in its possession unless it obtains the consent of the person to whom that sensitive personal information relates.

(2) Notwithstanding subsection (1), sensitive personal information may be processed–

(a) by a health care professional for the purposes of health and hospital care where it is necessary for–

(i) preventative medicine and the protection of public health;

(ii) medical diagnosis;

(iii) health care and treatment; and

(iv) the management of health and hospital care services;

(b) where it has been made public by the person to whom such information relates;

(c) for research and statistical purposes in accordance with section 43; and

(d) where the disclosure is required by written law.

(3) For the purpose of this section "health care professional" means a person registered under the–

(a) Medical Board Act;

(b) Dental Profession Act;

(c) Opticians Registration Act;

(d) Pharmacy Board Act; and
(e) Professions related to Medicine Act.

(4) A person who contravenes this section commits an offence.

75. (1) The head of an organization subject to a mandatory code of conduct, may upon the authorization of the Commissioner, disregard a request from an individual for access to that individual's personal information where it would unreasonably interfere with the operations of the organization because of the repetitious or systematic nature of the requests or the requests are frivolous or vexatious.

(2) Where an organization disregards a request under subsection (1) it shall notify the individual making the request.

76. Where an organization is subject to a mandatory code of conduct and an individual has a reasonable belief that the organization has within its custody or control personal information regarding that individual, the individual may–

(a) where the individual has requested access to or the correction of personal information held by an organization and the organization has refused such request, ask the Commissioner to conduct a review of the resulting decision, act or failure to act of the organization; or

(b) make a complaint to the Commissioner regarding an alleged failure of the organization to comply with the provisions of the mandatory code of conduct.

International Examples and Regional Harmonization

OECD

Use Limitation Principle

OECD (1980) 4 – Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the purpose specification principle except:

(a) with the consent of the data subject; or
(b) by the authority of law.

Security Safeguards Principle

OECD (1980) 5 – Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

Individual Participation Principle

OECD (1980) 7 – An individual should have the right:

(a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
(b) to have communicated to him, data relating to him within a reasonable time;

- at a charge, if any, that is not excessive;
- in a reasonable manner; and
- in a form that is readily intelligible to him;

(c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

(d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

United Nations

Guidelines Concerning Computerized Personal Data Files (1990)

UN (1990) Principle 4 – Everyone who offers proof of identity has the right to know whether information concerning him is being processed and to obtain it in an intelligible form, without undue delay or expense, and to have appropriate rectifications or erasures made in the case of unlawful, unnecessary or inaccurate entries and, when it is being communicated, to be informed of the addressees. Provision should be made for a remedy, if need be with the supervisory authority specified in principle 8 below. The cost of any rectification shall be borne by the person responsible for the file. It is desirable that the provisions of this principle should apply to everyone, irrespective of nationality or place of residence.

UN (1990) Principle 7 – Appropriate measures should be taken to protect the files against both natural dangers, such as accidental loss or destruction and human dangers, such as unauthorized access, fraudulent misuse of data or contamination by computer viruses.

European Union

PRINCIPLES RELATING TO DATA QUALITY

Article 6

1. Member States shall provide that personal data must be:

(a) processed fairly and lawfully;
(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with.

Article 7 –

Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
(d) processing is necessary in order to protect the vital interests of the data subject; or

Section III

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

Article 8 – The processing of special categories of data

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

2. Paragraph 1 shall not apply where:

(a) the data subject has given his explicit consent …or

(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law …or

(c) processing is necessary to protect the vital interests of the data subject …; or

(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a …other non-profit-seeking body with a political, philosophical, religious or trade-union aim …; or

(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional …

4. Subject to the provision of suitable safeguards, Member States may…, lay down exemptions in addition to those laid down in paragraph 2….

5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.

Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority.

6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.

7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

Article 12 – Right of access

Member States shall guarantee every data subject the right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:

– confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

Section III

- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,
- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

Article 14 – The data subject's right to object

Member States shall grant the data subject the right:

(a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

(b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).

Article 16 – Confidentiality of processing

Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

Article 17 – Security of processing

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

- the processor shall act only on instructions from the controller,
- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

Article 18 – Obligation to notify the supervisory authority

1. Member States shall provide that the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.

3.2.6 Disclosure of Personal Information

International Best Practices and Regional Trends:

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

Regional Examples

Antigua and Barbuda – NONE

Bahamas – GOOD – comprehensive framework in alignment with international best practice.

12.(1) A person, being a data controller shall, so far as regards the collection by him of personal data or information intended for inclusion in such data or his dealing with such data, owe a duty of care to the data subject concerned:

Provided that, for the purposes of this section, a data controller shall be deemed to have complied with the provisions of subsection (1)(b) of section 6 if and so long as the personal data concerned accurately record data or other information received or obtained by him from the data subject or a third party and include (and, if the data are disclosed, the disclosure is accompanied by) -

(a) an indication that the information constituting the data was received or obtained as aforesaid;

(b) if appropriate, an indication that the data subject has informed the data controller that he regards the information as inaccurate or not kept up to date; and

(c) any statement with which, pursuant to this Act, the data are supplemented.

(2) A data controller shall use contractual or other legal means to provide a comparable level of protection from any third party to whom he discloses information for the purpose of data processing.

Section III

In this Act any restrictions on or exceptions to the disclosure of personal data do not apply if the disclosure is -

(a) in the opinion of the Minister or the Minister of National Security required for the purpose of safeguarding the security of The Bahamas;
(b) required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders or assessing or collecting any tax, duty or other moneys owed or payable to the Government, statutory corporation, public body, or a local authority, in any case in which the application of those restrictions would be likely to prejudice any of the matters aforesaid;
(c) required in the interests of protecting the international relations of The Bahamas;
(d) required urgently to prevent injury or other damage to the health of a person or serious loss of or damage to property;
(e) required by or under any enactment or by a rule of law or order of a court;
(f) required for the purposes of obtaining legal advice or for the purposes of, or in the course of, legal proceedings in which the person making the disclosure is a party or a witness;
(g) made to the data subject concerned or to a person acting on his behalf; or
(h) made at the request or with the consent of the data subject or a person acting on his behalf.

17.(1) The Commissioner may, subject to the provisions of this section, prohibit the transfer of personal data from The Bahamas to a place outside The Bahamas, in such cases where there is a failure to provide protection either by contract or otherwise equivalent to that provided under this Act.

(2) In determining whether to prohibit a transfer of personal data under this section, the Commissioner shall also consider whether the transfer would be likely to cause damage or distress to any person and have regard to the desirability of facilitating international transfers of data.

(3) A prohibition under subsection (1) shall be effected by the service of a notice (referred to in this Act as a prohibition notice) on the person proposing to transfer the data concerned.

(4) A prohibition notice shall -

(a) prohibit the transfer concerned either absolutely or until the person aforesaid has taken such steps as are specified in the notice for protecting the interests of the data subjects concerned;
(b) specify the time when it is to take effect;
(c) specify the grounds for the prohibition; and
(d) subject to subsection (6), state that the person concerned may appeal to the Court under section 24 against the prohibition specified in the notice within twenty-one days from the service of the notice on him.

(5) Subject to subsection (6), the time specified in a prohibition notice for compliance with the prohibition specified therein shall not be expressed to expire before the end of the period of the twenty-one days specified in subsection (4) (d) and, if an appeal is brought against the prohibition, the prohibition need not be complied with and subsection (10) shall not apply in relation thereto, pending the determination or withdrawal of the appeal.

(6) If the Commissioner -

(a) by reason of special circumstances, is of the opinion that a prohibition specified in a prohibition notice should be complied with urgently; and
(b) such prohibition notice includes a statement to that effect,

subsections (4) (d) and (5) shall not apply in relation to the notice but the notice shall contain a statement of the effect of the provisions of section 24 (other than subsection (2)) and shall not require compliance with the prohibition before the end of the period of seven days beginning on the date on which the notice is served.

(7) The Commissioner may cancel a prohibition notice and, if he does so, shall notify in writing the person on whom it was served accordingly.

(8) This section shall not apply to a transfer of data if the transfer of the data or the information constituting the data is required or authorised by or under any enactment, or required by any convention or other instrument imposing an international obligation on The Bahamas, or otherwise made pursuant to the consent (express or implied) of the data subjects.

(9) This section applies, with any necessary modifications, to a transfer of information from The Bahamas to a place outside The Bahamas for conversion into personal data as it applies to a transfer of personal data from The Bahamas to such a place; and in this subsection "information" means information (not being data) relating to a living individual who can be identified from it.

(10) A person who, without reasonable excuse, fails or refuses to comply with a prohibition specified in a prohibition notice shall be guilty of an offence.

Barbados – POOR – The provisions do not treat with issues of collection and processing of information by the data controller. The provisions are limited to considerations of disclosure of information collected only.

[Electronic Transactions Act, CAP 308B, Part VI]

22. (1) Subject to this Part, no information that

(a) has been obtained under or by virtue of the provisions of this Act, and

(b) relates to the private affairs of a natural person or to any particular business,

shall, during the lifetime of that person or as long as that business continues to be carried on, be disclosed without the consent of that natural person or the person for the time being carrying on that business.

(2) Subsection (1) does not apply to any disclosure of information which is made

(a) for the purpose of facilitating the carrying out of any functions under Part IV;

(b) for the purpose of facilitating the carrying out of prescribed public functions of any persons;

(c) in connection with the investigation of any criminal offence or for the purposes of any criminal proceedings;

(d) for the purposes of any civil proceedings that

(i) relate to the provision of certification or accreditation services, and

(ii) are proceedings to which a person authorized in accordance with the provisions of Part IV is a party.

(3) In subsection (2)(*b*) "public functions" includes any function conferred by or in accordance with any provision contained in or ade under any enactment.

(4) If information is disclosed to the public in circumstances in which the disclosure does not contravene this section, this section shall not prevent its further disclosure by any person.

(5) Any person who discloses any information in contravention of this section is guilty of an offence and is liable

(a) on summary conviction, to a fine of $10 000;

Section III

(b) on conviction on indictment, to imprisonment for a term of 2 years or to a fine of $10 000 or to both.

(6) The Minister may make regulations prescribing standards for the processing of personal data whether that data originates within or outside of Barbados.

(7) The regulations may provide for
(a) the registration of the standards by data controllers and data processors;
(b) the establishment of a register that is available for public inspection, showing particulars of data controllers and data processors who have registered the standards and the dates thereof and the countries in respect of which the registration applies;
(c) the application of the standards to those countries specified in the regulations; and
(d) different standards to be applied in respect of personal data originating from different countries.

(8) A data controller or data processor who registers a standard referred to in subsection (6) must comply with the standard and any amendments made to that standard in respect of any personal data that
(a) originates from a country to which the standard applies; and
(b) is collected by the data controller during the period of registration.

(9) A data controller or data processor who contravenes subsection (8) is guilty of an offence and is liable on summary conviction to imprisonment for a term of 6 months or to a fine of $5 000 or to both.

Belize – NONE

Dominican Republic – NONE

Dominica, Grenada – NONE

Jamaica– NONE

St. Kitts and Nevis – LIMITED – Draft legislation is reported to be in preparation before presentation to Parliament, and is as such confidential. Copies of the draft were not available for assessment.

St. Lucia* – LIMITED (GOOD) – comprehensive framework in alignment with international best practice.

38. (1) A data controller shall not, without lawful excuse, disclose personal data in any manner that is incompatible with the purposes for which the personal data has been collected.

(2) Subject to subsection (4), a person shall not –
(a) obtain access to personal data, or obtain any information constituting such personal data, without prior authority of the data controller by whom the personal data is kept or disclose that personal data or information to another person.

(3) Subsection (2) shall not apply to a person who is an employee or agent of a data controller or processor and is acting within his mandate.

(4) A person shall not offer personal data for sale where the personal data has been obtained in breach of subsection (1).

(5) A data controller who contravenes this section commits an offence and is liable to a fine not exceeding twenty five thousand dollars or to imprisonment for a term not exceeding six months.

(6) For the purposes of subsection (5), an advertisement indicating that personal data is or may be for sale, constitutes an offer for the sale of personal data.

39. (1) Subject to subsection (2), a data controller shall not transfer personal data to a country or territory outside Saint Lucia unless-
(a) with the written consent of the Commissioner; and
(b) that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

(2) Subsection (1) (b) shall not apply where –
(a) the data subject has given his or her consent to the transfer;
(b) the transfer is necessary –
(i) for the performance of a contract between the data subject and the data controller, or for the taking of steps at the request of the data subject with a view to the data subject entering into a contract with the data controller;
(ii) for the conclusion of a contract between the data controller and a person, other than the data subject, which is entered at the request of the data subject, or is in the interest of the data subject, or for the performance of such a contract;
(iii) it is in the public interest or section 60 applies;.
(c) the transfer is made on such terms as may be approved by the Commissioner as ensuring the adequate safeguards for the protection of the rights of the data subject.

(3) For the purposes of section (2) (c), the adequacy of the level of safeguards of a country or territory shall be assessed in the light of all the circumstances surrounding the transfer of personal data, having regard in particular to –
(a) the nature of the personal data;
(b) the purpose and duration of the proposed processing;
(c) the country of origin and country of final destination;
(d) the rules of law, both general and sectoral, in force in the country in question; and
(e) any relevant codes of conduct or other rules and security measures which are complied with in that country or territory.

St. Vincent and the Grenadines – FAIR – While otherwise treating with the major considerations of data subject consent, and necessary exemptions, the provisions do not address the question of limiting transborder transfer of information.

11. (1) Subject to section 12, where a public authority holds personal information, it shall not disclose the information to a person, body or agency (other than the individual concerned), unless -
(a) the individual concerned has expressly or impliedly consented to the disclosure;
(b) the disclosure of the information is required or authorised by or under law;
(c) the disclosure of the information is one of the purposes in connection with which the information was collected, or is directly connected to that purpose;
(d) the individual concerned is reasonably likely to have been aware or made aware under section 8 (2) (c) that information of that kind is usually passed on to that person, body or agency;
(e) the information is to be disclosed -
(i) in a form in which the individual concerned is not identified; or
(ii) for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or
(f) the authority believes on reasonable grounds that disclosure of the information is necessary -
(i) to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or other person, or to public health or safety;

(ii) for the prevention, detection, investigation, prosecution or punishment of any offence or breach of law;
(iii) the enforcement of a law imposing a pecuniary or custodial penalty or both;
(iv) the protection of public revenue;
(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal; or
(vi) in the interests of national security.

(2) Any person, body or agency to whom personal information is disclosed under subsection (1) shall not use or disclose the information for a purpose other than the purpose for which the information was given to that person, body or agency.

12. A public authority shall only use or disclose personal information under section 10 or section 11, where such use or disclosure would not amount to an unreasonable invasion of privacy of the individual concerned, taking into account the specific nature of the personal information and the specific purpose for which it is to be so used or disclosed.

…

Trinidad and Tobago – LIMITED (GOOD) – comprehensive framework in alignment with international best practice.

41. Personal information under the custody or control of a public authority shall not be disclosed by the public authority in Trinidad and Tobago without the consent of the individual to whom it relates, except in accordance with sections 42, 43, 44 and 45.

42. Except as provided under any other written law, personal information under the control of a public authority may only be disclosed–

(a) for the purposes for which the information was collected or compiled by the public authority or for a use consistent with that purpose;
(b) for any purpose in accordance with any written law or any order made pursuant to such written law that authorizes such disclosure;
(c) for the purpose of complying with a subpoena or warrant issued or order made by a court, person or body with jurisdiction to compel the production of information or for the purpose of complying with rules of court relating to the production of information;
(d) to the Attorney General of Trinidad and Tobago for use in legal proceedings involving the State;
(e) to an investigative body specified by the Minister by Order, on the written request of the investigative body, for the purpose of investigating compliance with any written law or carrying out a lawful investigation, if the request specifies the purpose and describes the information to be provided;
(f) by one law enforcement agency in Trinidad and Tobago to another law enforcement agency within Trinidad and Tobago for the purpose of enforcement of a written law;
(g) to a law enforcement agency in a foreign country under a written agreement, treaty or under the authority of the Government of Trinidad and Tobago;
(h) if the head of the public authority agrees that a compelling circumstance exists that affects the health or safety of any person and if notice of the disclosure is mailed to the last known address of the individual to whom the information relates, unless the head of the public authority has a reasonable belief that providing notification could harm the health or safety of any person;
(i) so that the next of kin or friend of an injured, ill or deceased person may be contacted;
(j) for the purpose of collecting monies owing by an individual to the Government of Trinidad and Tobago or by a public authority to an individual;
(k) for statistical purposes where the disclosure meets the requirements of section 43; or

Section III

(l) for archival purposes where the disclosure meets the requirements of section 44.

43. A public authority may disclose personal information or may cause personal information in its custody or control to be disclosed for a research purpose, including statistical research only if–

(a) the research purpose cannot reasonably be accomplished unless that information is provided in individually identifiable form;

(b) the information is disclosed on condition that it not be used for the purpose of contacting a person to participate in research;

(c) any record linkage is not harmful to the individual to whom that information is about and the benefits to be derived from the record linkage are clearly in the public interest;

(d) the head of the public authority concerned has approved conditions relating to the following:

(i) security and confidentiality;

(ii) the removal or destruction of the individual identifiers at the earliest reasonable time;

(iii) the prohibition of any subsequent use or disclosure of that information in individually identifiable form without the express authorization of that public authority; and

(e) the person to whom that information is disclosed has signed an agreement to comply with the approved conditions, this Act and any of the public authority's policies and procedures relating to the confidentiality of personal information.

44. The archives of the Government of Trinidad and Tobago or the archives of a public authority may disclose personal information or cause personal information in its custody or control to be disclosed for archival or historical purposes if–

(a) the disclosure would not be an unreasonable invasion of professional or personal privacy;

(b) the disclosure is for historical research and is in accordance with section 42;

(c) the information concerns someone who has been deceased for twenty or more years; or

(d) the information is in a record that has been in existence for one hundred or more years.

45. Notwithstanding sections 42, 43 and 44, medical information may not be disclosed by a public authority except–

(a) with the consent of the person to whom such information relates; or

(b) by Order of the court.

46. (1) Where personal information under the custody and control of a public authority is to be disclosed to a party residing in another jurisdiction, the public authority shall inform the individual to whom it relates of the identity of–

(a) the person requesting the information; and

(b) the relevant public authority with responsibility for Data Protection in the other jurisdiction, and obtain his consent before disclosing the information.

(2) Where a person under subsection (1) does not consent to the release of his personal information, the public authority shall not so disclose.

(3) Subsections (1) and (2) shall not apply where the circumstances set out in section 41 exist, but personal information may be limited where the public authority determines that the jurisdiction to which the personal information is being sent does not have comparable standards.

(4) Where a person under subsection (1) consents to the release of his information and the public authority is–

(a) satisfied that the jurisdiction to which the information is being sent has comparable safeguards as provided by this Act, the public authority shall disclose the personal information;

(b) not satisfied that the jurisdiction to which the information is being sent has comparable safeguards, the public authority shall refer the matter to the Commissioner for a determination as to whether the other jurisdiction has comparable safeguards as provided by this Act and inform the individual to whom the personal information relates of the referral.

(5) Upon a referral under subsection (2) the Commissioner shall make a determination whether the other jurisdiction has or does not have comparable safeguards as provided by this Act, and inform the public authority accordingly.

(6) Where the public authority is informed that the jurisdiction to which the information is being sent–

(a) has comparable safeguards, the public authority shall inform the person concerned and disclose the personal information;

(b) does not have comparable safeguards, the public authority shall inform the person concerned and obtain his consent for the disclosure–

(i) without limitation; or

(ii) with limitation on the information sharing to the extent necessary to ensure the protection of personal privacy and information.

71. (1) Where a mandatory code of conduct is developed pursuant to section 70, it shall require at a minimum that personal information under the custody or control of an organization shall not be disclosed by that organization to any third party without the consent of the individual to whom it relates, except in general, where such information is disclosed for the purposes–

(a) for which the information was collected or for use consistent with that purpose;

(b) of a Court Order; or

(c) of complying with any written law.

(2) Where personal information under the custody and control of an organization is to be disclosed to a party residing in another jurisdiction, the organization shall inform the individual to whom it relates of the identity of–

(a) the person requesting the information; and

(b) the relevant public authority with responsibility for Data Protection in the other jurisdiction, and obtain his consent before disclosing the information.

(3) Where a person under subsection (2) does not consent to the release of his personal information, the organization shall not so disclose.

(4) Where a person under subsection (2) consents to the disclosure of his information and the organization is–

(a) satisfied that the jurisdiction to which the information is being sent has comparable safeguards as provided by this Act, the organization shall disclose the personal information;

(b) not satisfied that the jurisdiction to which the information is being sent has comparable safeguards, the organization shall refer the matter to the Commissioner for a determination as to whether the other jurisdiction has comparable safeguards as provided by this Act and inform the individual to whom the personal information relates of the referral.

(5) Upon a referral under subsection (4) the Commissioner shall make a determination whether the other jurisdiction has or does not have comparable safeguards as provided by this Act, and inform the organization accordingly.

(6) Where the organization is informed that the jurisdiction to which the information is being sent–

(a) has comparable safeguards, the organization shall inform the person concerned and disclose the personal information;

Section III

(b) does not have comparable safeguards, the organization shall inform the person concerned and obtain his consent for the disclosure–

(i) without limitation on the personal information; or

(ii) with limitation on the personal information sharing to the extent necessary to ensure the protection of personal privacy and information.

International Examples and Regional Harmonization

OECD

Article 10 – Use Limitation Principle

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) with the consent of the data subject; or

b) by the authority of law.

United Nations

Guidelines Concerning Computerized Personal Data Files (1990)

Article 3 – Principle of the purpose- specification

The purpose which a file is to serve and its utilization in terms of that purpose should be specified, legitimate and, when it is established, receive a certain amount of publicity or be brought to the attention of the person concerned, in order to make it possible subsequently to ensure that:

- …;
- None of the said personal data is used or disclosed, except with the consent of the person concerned, for purposes incompatible with those specified;
- …

Article 6 – Power to make exceptions

Departures from principles 1 to 4 may be authorized only if they are necessary to protect national security, public order, public health or morality, as well as, inter alia, the rights and freedoms of others, especially persons being persecuted (humanitarian clause) provided that such departures are expressly specified in a law or equivalent regulation promulgated in accordance with the internal legal system which expressly states their limits and sets forth appropriate safeguards.

Exceptions to principle 5 relating to the prohibition of discrimination, in addition to being subject to the same safeguards as those prescribed for exceptions to principles 1 and 4, may be authorized only within the limits prescribed by the International Bill of Human Rights and the other relevant instruments in the field of protection of human rights and the prevention of discrimination.

European Union

INFORMATION TO BE GIVEN TO THE DATA SUBJECT

Article 10 – Information in cases of collection of data from the data subject

Section III

Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;
(b) the purposes of the processing for which the data are intended;
(c) any further information such as
  – the recipients or categories of recipients of the data,
  – whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
  – the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Information where the data have not been obtained from the data subject

1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;
(b) the purposes of the processing;
(c) any further information such as
  – the categories of data concerned,
  – the recipients or categories of recipients,
  – the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.

Article 13 – Exemptions and restrictions

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:

(a) national security;
(b) defence;
(c) public security;
(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
(g) the protection of the data subject or of the rights and freedoms of others.

2. Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

3.3 Summary of Assessment of Regional Texts

Provided on the overleaf is a summary of the major findings coming out of the comparisons undertaken in Section 7 above.

In short, it can be said that the frameworks analyzed do generally well in the implementation of the core functional objectives of the Privacy and Data Protection. That is to say, that the provisions are creditable when considering concerns such as the collection, use and disclosure of personal information.

There seems to be some significant variance in the model of administrative governance proposed. This suggests that harmonization will hinge largely on political negotiation at the regional level to facilitate a common view point of the institutional context of the oversight body, the Data Commissioner. Recommendations for the ongoing development of Data Protection Frameworks across the region can be summarized as follows:

- 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 appropriate definition of 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 identifying Data Controllers, and whether that recognition should be facilitated through either the registration of data controllers, or should the establishment of a generally applicable obligation on industry and relevant public authorities**.**

Summary Chart of Key Elements and Status

Country/Region	1. Legal Mandate	2. Institutional Framework	3. Regulatory Empowerment	4. Collection of Personal Information	5. Storage and Use of Information	6. Disclosure of Information
Antigua and Barbuda	NONE	NONE	NONE	NONE	NONE	NONE
Bahamas	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD
Barbados	POOR	NONE	NONE	NONE	NONE	POOR
Belize	NONE	NONE	NONE	NONE	NONE	NONE
Dominica	NONE	NONE	NONE	NONE	NONE	NONE
Dominican Republic	NONE	NONE	NONE	NONE	NONE	NONE
Grenada	NONE	NONE	NONE	NONE	NONE	NONE
Guyana	NONE	NONE	NONE	NONE	NONE	NONE
Haiti	NONE	NONE	NONE	NONE	NONE	NONE
Jamaica	NONE	NONE	NONE	NONE	NONE	NONE
St. Kitts and Nevis	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED
St. Lucia*	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED
St. Vincent and the Grenadines	FAIR	POOR	FAIR	GOOD	FAIR	FAIR
Suriname	NONE	NONE	NONE	NONE	NONE	NONE
Trinidad and Tobago*	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED

* Bills laid before Parliament, not yet passed as statute.

ANNEXES

Annex 1: Bibliography

1. Christopher Millar, Communications Privacy, in Telecommunications Law and Regulation, (Jan Walden and John Angel eds., 2005), at 381.
2. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (EU Data Protection Directive).
3. Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications).
4. See the Privacy Commissioner's report into the operation of the private sector provisions of the Privacy Act 1988. Office of the Privacy Commissioner, Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988, March 2005, available at www.privacy.gov.au/act/review/revreport.pdf.
5. Harmonisation of the Legal Framework Governing ICTs in West African States, Economic Community of West African States, United Nations Economic Commission for Africa, West African Economic and Monetary Union, by Abdoullah CISSE, University Professor Consultant July 2007
6. United Nations Conference on Trade and Development, Information Economy Report 2007-2008, Science and technology for development: the new paradigm of ICT
7. Prepared by the UNCTAD Secretariat UNITED NATIONS New York and Geneva, 2007
8. 13th Meeting of the Intergovernmental Committee of Experts (ICE), Mahe, Seychelles, 27-29 April 2009 Ad Hoc Expert Group Meeting : "Harmonization of ICTs Policies and Programmes in Eastern Africa Subregion and Prospects" , United Nations Economic Commission for Africa Subregional Office for Eastern Africa.CA
9. International Telecommunication Union. Cybercrime Legislation Resources, ITU Toolkit for Cybercrime legislation, developed through the American Bar Association's Privacy & Computer Crime Committee Section of Science & Technology Law with Global Participation, ICT Applications and Cybersecurity Division Policies and Strategies Department, ITU Telecommunication Development Sector, Draft April 2009, www.itu.int/ITU-D/cyb/
10. Annex 4 Contribution by Professor Michael Geist University of Ottawa, Faculty of Law, Director of E-commerce Law, Goodmans LLP, found on www.itu.int/ITU-T/special-projects/ip-policy/final/Attach04.doc
11. Data Protection (Privacy of personal Information Bill), Bahamas, available at http://laws.bahamas.gov.bs/annuals/No3of2003style.html
12. Privacy and Personal Information Bill, Dominica, available at www.sfa2005.eu/sites/default/files/Dominica
13. Data Protection Act 1998, UK Explained, www.legislation.org.uk/
14. Data Protection Act UK, www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1
15. Information Commissioner's Office Website, www.ico.gov.uk.
16. Malta Data Protection Act- found at www.sfa2005.eu/sites/default/files/Malta%20Data%20Protection%20Act.pdf

Annex 1

Additional Websites

17. www.ictregulationtoolkit.org/en/Section.2107.html
18. www.itu.int/osg/spu/ni/ubiquitous/Presentations/10_lam_dataprotection.pdf
19. http://peterfleischer.blogspot.com/2009/01/launching-another-global-forum-to-talk.html
20. www.privacyconference2008.org/adopted_resolutions/STRASBOURG2008/resolution_international_standards_en.pdf
21. www.itu-coe.ofta.gov.hk/vtm/ict/faq/q10.htm
22. www.oecd.org/document/18/0,2340,en_2649_34255_1815186_119820_1_1_1,00.html
23. www.itu.int/dms_pub/itu-t/oth/23/01/T23010000060002PDFE.pdf
24. www.itu.int/ITU-T/newslog/New+Report+On+Lawful+Interception.aspxhttp://www.itu.int/ITU-

Annex 2:

Participants of the First Consultation Workshop for HIPCAR Project Working Group dealing with ICT Legislative Framework – Information Society Issues
Gros Islet, Saint Lucia, 8-12 March 2010

Officially Designated Participants and Observers

Country	Organization	Last Name	First Name
Antigua and Barbuda	Ministry of Information, Broadcasting, Telecommunications, Science & Technology	SAMUEL	Clement
Bahamas	Utilities Regulation & Competition Authority	DORSETT	Donavon
Barbados	Ministry of Finance, Investment, Telecommunications and Energy	BOURNE	Reginald
Barbados	Ministry of Trade, Industry and Commerce	COPPIN	Chesterfield
Barbados	Cable & Wireless (Barbados) Ltd.	MEDFORD	Glenda E.
Barbados	Ministry of Trade, Industry and Commerce	NICHOLLS	Anthony
Belize	Public Utilities Commission	SMITH	Kingsley
Grenada	National Telecommunications Regulatory Commission	FERGUSON	Ruggles
Grenada	National Telecommunications Regulatory Commission	ROBERTS	Vincent
Guyana	Public Utilities Commission	PERSAUD	Vidiahar
Guyana	Office of the Prime Minister	RAMOTAR	Alexei
Guyana	National Frequency Management Unit	SINGH	Valmikki
Jamaica	University of the West Indies	DUNN	Hopeton S.
Jamaica	LIME	SUTHERLAND CAMPBELL	Melesia
Saint Kitts and Nevis	Ministry of Information and Technology	BOWRIN	Pierre G.
Saint Kitts and Nevis	Ministry of the Attorney General, Justice and Legal Affairs	POWELL WILLIAMS	Tashna
Saint Kitts and Nevis	Ministry of Youth Empowerment, Sports, Information Technology, Telecommunications and Post	WHARTON	Wesley
Saint Lucia	Ministry of Communications, Works, Transport and Public Utilities	FELICIEN	Barrymore
Saint Lucia	Ministry of Communications, Works, Transport and Public Utilities	FLOOD	Michael R.
Saint Lucia	Ministry of Communications, Works, Transport and Public Utilities	JEAN	Allison A.
Saint Vincent and the Grenadines	Ministry of Telecommunications, Science, Technology and Industry	ALEXANDER	K. Andre
Saint Vincent and the Grenadines	Ministry of Telecommunications, Science, Technology and Industry	FRASER	Suenel
Suriname	Telecommunicatie Autoriteit Suriname / Telecommunication Authority Suriname	LETER	Meredith
Suriname	Ministry of Justice and Police, Department of Legislation	SITALDIN	Randhir

Annex 2

Country	Organization	Last Name	First Name
Trinidad and Tobago	Ministry of Public Administration, Legal Services Division	MAHARAJ	Vashti
Trinidad and Tobago	Telecommunications Authority of Trinidad and Tobago	PHILIP	Corinne
Trinidad and Tobago	Ministry of Public Administration, ICT Secretariat	SWIFT	Kevon

Regional / International Organizations' Participants

Organization	Last Name	First Name
Caribbean Community Secretariat (CARICOM)	JOSEPH	Simone
Caribbean ICT Virtual Community (CIVIC)	GEORGE	Gerry
Caribbean ICT Virtual Community (CIVIC)	WILLIAMS	Deirdre
Caribbean Telecommunications Union (CTU)	WILSON	Selby
Delegation of the European Commission to Barbados and the Eastern Caribbean (EC)	HJALMEFJORD	Bo
Eastern Caribbean Telecommunications Authority (ECTEL)	CHARLES	Embert
Eastern Caribbean Telecommunications Authority (ECTEL)	GILCHRIST	John
Eastern Caribbean Telecommunications Authority (ECTEL)	HECTOR	Cheryl
International Telecommunication Union (ITU)	CROSS	Philip
International Telecommunication Union (ITU)	LUDWIG	Kerstin
Office of Trade Negotiations (formerly CRNM) Caribbean Community Secretariat (CARICOM)	BROWNE	Derek E.
Organization of Eastern Caribbean States Secretariat (OECS)	FRANCIS	Karlene

HIPCAR Project Experts

Last Name	First Name
MARTÍNS DE ALMEIDA	Gilberto
GERCKE	Marco
MORGAN[14]	J Paul
PRESCOD	Kwesi

[14] Workshop Chairperson