fastforward

Trinidad and Tobago. Accelerating into the digital future.

Ministry of Public Administration
& Information

"NATIONAL POLICY ON DATA PROTECTION."

December 2005

Table of Contents

1.0 Introduction

The Ministry of Public Administration and Information (MPAI), through extensive consultation with the public sector, the private sector and academia, developed ***fastforward***, the National Information and Communications Technology (ICT) Strategy for Trinidad and Tobago. ***fastforward*** is a comprehensive plan to leverage the power of people, innovation, education, information technology and infrastructure to accelerate social, economic and cultural development for all elements of society.

fastforward is the National Information and Communications Technology (ICT) Strategy for Trinidad and Tobago. It complements and builds upon Vision 2020, the national development plan, and will play a central role in Trinidad and Tobago becoming a knowledge-based society and achieving its goal of developed country status by the year 2020.

The objectives of ***fastforward*** are to:

- Provide all citizens with affordable Internet access,
- Focus on the development of children, and skills of adults to ensure a sustainable solution and a vibrant future,
- Promote citizen trust, access, and interaction through good governance, and
- Maximise the potential within all citizens, and accelerate innovation, to develop a knowledge-based society.

Substantial legal and policy change is anticipated as part of Trinidad and Tobago's evolution toward a knowledge-based economy. Liberalization of the telecommunications industry will take place, rules relating to electronic information handling must be clarified, and citizen privacy and security must be ensured. Consequently, government has an important role to play in ensuring there is a clear and stable policy and a regulatory and legal infrastructure in place that supports the smooth transition and continuous progression of the country's ICT programmes.

In 1999, the Attorney General instructed the Law Commission of Trinidad and Tobago to prepare a legislative package on electronic commerce. To date, two of the three Bills comprising that package are now Acts: the *Computer Misuse Act, 2000*, and the *Electronic Transfer of Funds Crime Act, 2000*. Two additional policies and bills are necessary at this stage to facilitate social and economic development through the use of ICT: the Electronic Transaction Policy and Bill and the Data Protection Policy and Bill. These Policies would provide the principles that guide the completion of the respective Bills. This document focuses on Data Protection Policy and Bill.

2.0 Background

2.1 What is Data Protection?

Data protection is a broad term and can relate to the physical security of the data, protection from theft and hackers or illicit changes to data, ensuring that data is disposed of properly, ensuring that only authorized people have access to data, ensuring that the data is accurate, that it maintains its integrity both technically and in the purposes for which it is being used, and that the purposes for which it is used are authorized, predictable and do not cause harm. This covers a lot of ***area*** and any Policy or legislation that purports to deal with all these matters will need to be accompanied by a significant number of guidance documents and regulations clarifying the specific requirements of the general policies.

Yet these are, in one form or another, the concerns to be addressed by a Policy on Data Protection. These matters are all inter-related and they are not new. Mankind has taken measures to protect information since we learned that it had value to us. But protection of data, and particularly personal data, has become more important. There is more personal data in circulation and more uses to which it can be put. There are new forms of data—DNA, genetic profiling, results of new physical and psychological testing. Computers allow for storage, manipulation, matching, mining and transmission across jurisdictional lines in ways that could not have been predicted even fifty years ago. Citizens, whether speaking as individuals or as consumers, have become increasingly concerned about what information is held about them by governments, businesses and others.

The Government of Trinidad and Tobago, as part of its initiative to use ICT to enhance economic growth and bring new benefits to citizens, must address the issue of data protection. Both the State and individuals carrying on business in Trinidad and Tobago must be able to assure individuals whose personal information is held in our data systems (usually, but not necessarily, a computer) that their data is being used for the expected purposes, that it is physically safe, that it cannot be picked up by someone in the garbage in the back alley or faxed to a stranger in another country. Those assurances can be given only if we have a systematic approach to the protection of data in place.

2.2 Why is a Data Protection Policy Necessary?

Privacy has long been understood to have a value in a civil society that respects the inherent rights and values of mankind. The Constitution of Trinidad and Tobago recognises the right to privacy as an individual and within a family. The Universal Declaration of Human Rights states that privacy is a fundamental human right. Most Western countries have in place legislation and legal precedents that protect the right of an individual to privacy and the right to maintain certain types of information (often called “sensitive information”) as private and personal.

Privacy has always been a concern. Laws dealing with trespass and the need for search warrants, for example, recognise that we have a right to be “left alone.” In polite society it is often considered inappropriate to question people too closely about their religious or political beliefs or personal habits or income. Revealing information about one’s self is a step on the way to forming a friendship and is generally both consensual and mutual. We reveal information about ourselves for particular purposes—to our doctor, our banker, or our accountant. But we have expectations about the use of the information and expectations that it will be kept confidential. Indeed, certain professions, like the medical or legal professions, have professional codes that impose confidentiality requirements on practitioners. But these arrangements are now under threat and are increasingly being found to be inadequate to protect individuals and society from new forms of privacy invasion.

For example, computers and information technology raise new threats to privacy, however. Thus

- They facilitate the collection and maintenance of extensive record systems and the retention of data on those systems;
- They make data easily and quickly accessible from many distant points;
- They make it possible for data to be transferred quickly from one information system to another and one jurisdiction to another; and
- They make it possible for data to be combined in ways that might not be otherwise practicable and yet yields entirely new and in-depth information about an individual.

Privacy is also taking on a new importance in medicine and related disciplines. New genetic advances, for example, can predict future illnesses or susceptibilities to particular illnesses. Knowledge of these potential illnesses can have an impact on individual welfare, availability of insurance and employment, acceptance in society, and research into possible cures. Some illnesses carry social stigmas yet at the same time have implications for broader management of public health. Privacy protection plays a role in all these larger policy issues and it is important that the country begin to tackle these issues taking into account the values of privacy. In addition, if we want to take advantages of the benefits that ICT can offer to improve health care through tele-health initiatives, the computerization of health records, e-Health programmes, and so on, a privacy policy will be a necessary component to encourage co-operation, assure professionals that they are continuing to meet their professional obligations, and avoid costly and embarrassing errors.

There are also specific international pressures for improvement of privacy protection being placed on Trinidad and Tobago if it wishes to reach its potential as a player in the global economy. The first international attempt to develop principles to deal with the protection of personal privacy in the context of computer data and the potential for trans-border flows of personal information was the 1980 Guidelines developed by the Organisation for Economic Co-operation and Development (OECD).

The OECD Guidelines were also reflected in the European Community Parliament and Council *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*. Noting that data processing systems are intended to be servants and must respect fundamental rights of individuals, including privacy, the Directive sets out Principles Relating to Data Quality. Chapter IV, Transfer of Personal Data to Third Countries, sets out the provisions that have critical implications for non-EC countries, including Trinidad and Tobago. The first principle of Article 25 states:

> "The Member State shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection".

The EC Directive, coupled with the Principles outlined in the OECD Guidelines, have informed most of the legislation and practice in privacy protection in developed and developing countries, including this Policy and Bill. The legislative and institutional form of privacy protection may vary significantly, however. The primary differences are not in the underlying principles but in the degree to which industry takes responsibility for implementation and the degree to which coverage applies across commercial and government sectors.

Most countries, with the exception of the United States, have set up data protection agencies (i.e., Data Protection Commissioners, Privacy Commissioners) with varying degrees of oversight, enforcement power, and regulatory or advisory powers. In some regimes, self-regulation through industry codes of practice plays a stronger role than in others. The OECD has noted that the privacy protection systems in many countries are hybrid approaches, combining self-regulation and legislative action, although the issue has often been approached as if these approaches are entirely separate.

In fact, a combination of policy tools often leads to the strongest result and this may be particularly true in Trinidad and Tobago, which wishes to be able to deal at a sophisticated level and become a leader in connectivity and ecommerce in the Caribbean, while focusing on priorities and using resources wisely. Privacy protection is an area where the Government can provide leadership and guidance through information (using e-Government and other information and distribution media); early adoption of privacy-enhancing technology, techniques and policies; selective legislation in key sectors (such as financial services and health); and promotion of contractual safeguards and dispute settlement mechanisms. In addition, key regulators and self-governing professional bodies can play an important role in fostering privacy principles and applications through a network of both regulatory requirements and internal compliance policies.

2.3 Government Protection of Personal Privacy

The Policy and Bill have specific provisions relating to the holding and use of personal information by ***government authorities.*** The definition of public authorities is essentially the same as that used in the Freedom of Information Act, 1999 and covers a wide range of organisations and entities. The purpose of addressing ***government's*** use of personal information is two-fold. First, public authorities are the primary holders of personal information ***in the country***, in one form or another, and may also use the power of the state to collect other information. Tax records, birth and death records, health records, business records can all be found under the administration of a government body. It is important that Government's data banks and use of personal information be subject to a transparent and accountable regime with an objective of balancing personal information protection needs with what may from time to time be broader public interest needs, such as law enforcement, security, or public health. The Policy and Bill provide an infrastructure for accountable decision-making in these areas. It is important, therefore, that the Policy and Bill deal with Government and Government's role in data protection and the protection of the privacy of the individual.

The second reason why Government should be subject to the Policy and Bill is the importance of Government playing a leadership role in developing a new ethic and way of thinking about personal privacy. Many individuals shrug their shoulders and say, "I have nothing to hide." In the normal course of events, that may be very true. But they underestimate the power of modern data collection and data matching or data mining and the uses to which such information can be put. Marketers or others can develop highly detailed profiles of individuals—their likes, dislikes, dreams, wants, personal habits (eating, reading, sexual preferences, personal care, etc.). We may assume we have nothing to hide partly because we assume those deeply personal matters that might embarrass us if made public are really private and only think of the more obviously public matters that are not widely known, but are known among our neighbours and friends—brand of our car or the number of times we have pizzas delivered.

As a leader, Government will have a role in alerting and educating citizens and consumers to the areas in which their privacy might be compromised. Citizens must know what they should demand from the businesses they deal with in terms of privacy protection (which, in turn, may strengthen the effectiveness of a voluntary code of practice dealing with personal privacy put in place by a business dealing with consumers). Government will also be able to pass on its own experience and lessons learned in implementing the Policy and Bill to the private sector, whether the private sector is dealing with a mandatory code of conduct or is merely trying to implement best practices through a voluntary code.

2.4 Linkages with other Laws

Rights to privacy are enshrined at the constitutional level and the intent of the Data Protection Policy is to remove impediments from existing legislation to the protection of personal information

and to ensure that no new barriers are created with new legislation that is developed. The data protection policy should address privacy issues that were not covered in the following legislation:

- Law of contracting and the commercial code,
- Evidence Act and admissibility and validity of electronic transactions,
- Computer Misuse Act,
- Intellectual Property,
- Consumer Protection,
- Laws on Electronic Transactions,
- Laws to Protect Company Information.

Privacy, which among other definitions, has been called "the right to be left alone," becomes an important element in the control of other electronic activities. Specifically, unsolicited marketing, automated calling, telemarketing, fax marketing, and "spam," Data protection legislation or telecommunications legislation in a number of jurisdiction deals with these electronic activities. The codes of conduct developed, for example, Internet Service Providers and intermediaries, pursuant to this Policy and Bill, as well as the Policy and Bill on Electronic Transactions, will be part of a more general Government approach to dealing with the dangers and costs of "spam." For example, it is this Policy and Bill that will deal with the practice of "data harvesting" from computers or the placement of "spyware" without permission.

2.5 Policy Objectives

This Policy and Bill are aligned with the objectives of Vision 2020 and relate specifically to achieving the Public Utilities and infrastructure goals, both of which address Information and Communications Technology, including telecommunications.

The Vision 2020 Focus on infrastructure addresses the National information and Communication policy objectives, which are to:

- Encourage competition in telecommunications;
- Establish an authority to facilitate information gathering and dissemination systems;
- Decentralize access to information and improve data collection;
- Encourage a culture of research and development;
- Enact legislation for facilitate implementation of the above;
- Amend antiquated laws to support the use of available technology and dissemination of information; and
- Encourage the formation of private sector data collection services.

In order to achieve these objectives in a political, social, and legal context that balances the entrepreneurial development goals against the needs of individuals to protect their privacy and maintain the integrity of their private lives, a Policy and Bill on Data Protection is required.

The main purpose of this Policy is to;

- **Protect the individuals' right to privacy:** Privacy is a fundamental human right and this policy recognises that respect for privacy is viewed as a prerequisite to enable citizens to fully develop as individuals as well as to participate in society. It is recognised that the Government of the Republic of Trinidad and Tobago must play a key role in protecting this right.

- **Provide adequate protection of personal information:** the General Privacy Principles establish norms and requirements for the physical and electronic security of personal information, for developing protocols to ensure that the information is accurate and used correctly including limiting access to persons who have no right to the information. These

are practical measures that will have an effect on how government and business treats personal information and will require the development of internal procedures and protocols, as well as the possible installation of protective devices, firewalls and so on. This aspect of the Policy is intended to ensure that the broader objectives of protection and appropriate uses are backed by the necessary actions that provide the practical protection needed to fulfill the other objectives.

- **Provide Promote electronic commerce:** Promoting confidence and trust in ecommerce is important to the success of any ecommerce initiative. Many countries have developed or are currently developing laws in an effort to promote electronic commerce. These countries recognise that consumers are uneasy with the increased availability of their personal data, particularly with new means of identification and forms of transactions and with their personal information being sent worldwide. Privacy laws are being introduced as part of a package of laws intended to facilitate electronic commerce by setting up uniform rules.

- **Create obstacles to electronic crime:** Given the rapid development of telecommunications networks and the pervasiveness of ICT, the occurrence of electronic crimes has grown. Electronic crimes have been spurred on by the rapid manipulation, transborder transfer, storage and capture of electronic data, all posing a threat to personal privacy. Thus, this policy is important tool in the fight against electronic crime.

- **Enable trade:** This policy aims to enable trade; inadequate data protection is a barrier to conducting trade with countries, particularly the EU and in the Pacific, which require that personal data be protected. Trinidad and Tobago is a multicultural and multiracial society and thus there is a need to mange diversity when designing policies. Our citizens and companies are interested in conducting trade with a multitude of companies globally. As such, policies adopted should be enabling and consider the requirements of the variety a trading partners, countries and sectors.

- **Harmonise with international standards**: Western democracies generally have legislation in place that recognise the importance and need to protect individual information and personal privacy. In some cases, such as within the EU, maintaining comparable standards becomes an issue for ability to carry on trade. But more importantly, having comparable standards is a sign of membership in an international community that recognises and honours certain values. These values are compatible with the values of Trinidad and Tobago (and found in our constitution) and should be expressed explicitly through Policy and legislation.

- **Meet compliance with target market laws:** In addition, it is important for Trinidad and Tobago to adopt adequate data protection laws to be compliant with target market laws in various sectors such as the US *Health Insurance Portability and Accountability Act* (HIPAA). Thus it is important for this policy to meet compliance with privacy standards in various sectors such as the health and financial sector.

- **Establish a national Data Commissioner.** This Policy and Bill recognise the need for a credible, expert institutional infrastructure to advise the Government on the implementation of this Policy and Bill, as well as determine issues of compliance and redress. It recommends that a regulatory body be established in the form of a Data Commissioner whose role would be to hear appeals regarding access and correction of personal information held by public authorities, and promote the purposes of the legislation through education, research, and co-operative activities.

- **Encourage development of industry or sector specific codes of conduct**, including mechanisms for dispute resolution by industry bodies. The Policy and Bill will recognise

roles for industry regulators to allow sectoral expertise to be applied to data protection issues within an industry and prevent unnecessary duplication of compliance efforts.

A draft Data Protection Bill was developed by the Attorney General's Department in 2003 as part of a legislative package on Electronic Commerce. This was drafted on recommendation of the National E-Commerce Policy Committee. Since then, the government created ***fastforward*** and the Vision 2020 plans which intend to holistically drive the coordinated social and economic development of Trinidad and Tobago and use ICTs as a major catalyst for growth,

The Government has decided to revisit the legislation to ensure compatibility with recent developments in the area of Information and Communications Technologies, as well as alignment with national development policy. The approach and principles adopted were selected based on their ability to meet the key objectives of this policy. In general, the main criteria was the protection of personal information, the ability to serve as an enabler to the development of the e-economy rather than a hindrance, while at the same time providing an adequate level of protection that is required by trade partners and target sectors**.**

2.6 Legislative Approach

The approach taken in the Data Protection Policy and Bill is flexible, taking into account both the need to have principles in place that will provide assurances to the citizens of Trinidad and Tobago and people who do business with Trinidad and Tobago that rights to personal privacy are respected and the need to ensure that the regulatory regime does not overwhelm the public and private sectors with new responsibilities that are unrealistic and burdensome.

Following a model that uses the Government of Trinidad and Tobago as the leader in the protection of personal privacy, the Policy and the Bill make privacy protection by public authorities mandatory. The protection of personal privacy has always had a high value in Trinidad and Tobago—indeed it is value enshrined in the Constitution—and it has been implicitly recognised in the Freedom of Information Act, 1999. While citizens have a right to information about their government, this right must be balanced with the rights of individuals to maintain and respect personal privacy. The Data Protection Policy and Bill clarify and extend these rights. Thus, Government is subject to specific responsibilities regarding data sharing and data matching that recognise the importance of Government as a holder of information about individuals.

The Policy and Bill provides for a Data Commissioner to deal with complaints and appeals from decisions made by heads of public authorities about personal information and requests by individuals for access to their own information or correction of that information. The Data Commissioner provides a credible source of expertise, authoritative decision-making, and disinterested resolution of disputes. It is likely that the decisions and guidance of the Data Commissioner dealing with data protection by Government will provide the leadership that will be needed to integrate the values of privacy protection into the business values of the private sector in Trinidad and Tobago.

With respect to the private sector, the Policy and Bill emphasize the importance of the Privacy Protection Principles. These Principles represent good business practice and should be promoted as part of the general business ethic of the country and part of what aware consumers should expect of businesses to which they entrust their personal information. The Policy and Bill therefore stress education and promotion as important elements of successfully integrating the Privacy Protection Principles into the daily life of citizens.

The Data Protection Commissioner will have a role in promoting these values, as will other stakeholders, such as industry organisations, industry regulators, consumer protection agencies and Government as a whole. To promote more focused acceptance and adherence to the Principles, it is expected that industry groups or even individual larger corporations will develop

codes of conduct that will translate the higher level Privacy Protection Principles into more detailed compliance policies that will reflect the needs of particular industries, the type of information they collect and the needs of their customers. For example, a bank will have different concerns about what constitutes consent of a customer to use information than will a newspaper dealing with subscribers. Medical practitioners and their patients have different needs and concerns than telephone subscribers. Codes of conduct allow groups to particularize the Privacy Protection Principles and establish mechanisms for dispute resolution, among other matters. To maintain a consistent application and interpretation of the requirements of the Privacy Protection Principles, the Policy and Bill provide a mechanism for the Commissioner to approve codes of conduct, taking into account certain criteria including avoidance of anti-competitive conduct.

The general approach of the Policy and Bill is promotion of the General Privacy Protection Principles and voluntary development of codes of conduct among private sector groups, organisations, or industries. In some cases, however, the protection of personal privacy and personal information will be so important that voluntary development of codes of conduct or voluntary compliance will not be sufficient to either protect individuals or create the environment of trust and confidence that is needed for Trinidad and Tobago to interact globally. In these cases, the Policy and Bill create a structure that will allow the Data Commissioner to require the development of codes of conduct and impose a time limit on development to avoid delay. Some of the areas that might be subject to mandatory codes of conduct include the health sector, the financial services sector, credit agencies, and regulated professions (e.g., accounting and health care professions).

Although a number of health authorities might generally be considered to be public authorities and subject to the provisions of the Policy and Bill relating to Government, the protection of personal information in the health sector has a number of special issues attached to it. The general Principles of Privacy Protection apply, but matters relating to consent, for example, require particular care depending on the situation. For this reason, the Policy and Bill are structured to allow issues relating to protection of personal privacy in medical records and the health care system generally to be dealt with on a more specific and targeted basis.

In selected cases—most likely those where the development of a code of conduct has been mandated—the Minister may make the application of a code mandatory by an order that is placed before the House and subject to a negative resolution of the House. The Data Commissioner would play a role similar to that which he would play for the Government with respect to the mandatory private sector codes by hearing appeals and reviewing decisions and data protection practices.

In sum, the legislative approach taken in the Policy and Bill is a combination of the voluntary and mandatory with Government taking a leadership role in ensuring that the citizen's right to privacy is protected and promoted. This Policy and Bill take a ***sectoral approach*** to data protection, which is appropriate for developing countries such as Trinidad and Tobago as it allows for innovation in various sectors and is not as restrictive and costly as the comprehensive approach. This approach is adopted by countries in North America and the Caribbean which are some of Trinidad and Tobago's major trading partners.

The Trinidad and Tobago Policy and Bill on Data Protection draws on a number of sources, including the OECD Guidelines, the EU Directive, the Canadian Standards Association Standard on Protection of Personal Privacy, and legislation in a number of jurisdictions, including Canada, Canadian provinces, New Zealand, Australia, the United Kingdom, and Ireland.

3.0 Principles of the Data Protection Policy and Bill

Part I: General Principles of Protection of Personal Privacy

3.1 Principle 1: Accountability

An organisation is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organisation's compliance with the following principles:

3.1.1 Accountability for the organisation's compliance with the principles rests with the designated individual(s), even though other individuals within the organisation may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organisation may be delegated to act on behalf of the designated individual(s).

3.1.2 The identity of the individual(s) designated by the organisation to oversee the organisation's compliance with the principles shall be made known upon request.

3.1.3 An organisation is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organisation shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

3.1.4 Organisations shall implement policies and practices to give effect to the principles, including; implementing procedures to protect personal information; establishing procedures to receive and respond to complaints and inquiries; training staff and communicating to staff information about the organisation's policies and practices; and developing information to explain the organisation's policies and procedures.

3.2 Principle 2: Identifying Purposes

The purposes for which personal information is collected shall be identified by the organisation at or before the time the information is collected.

3.2.1 The organisation shall document the purposes for which personal information is collected in order to comply with the Openness principle (Clause 3.8) and the Individual Access principle (Clause 3.9).

3.2.2 Identifying the purposes for which personal information is collected at or before the time of collection allows organisations to determine the information they need to collect to fulfill these purposes. The Limiting Collection principle (Clause 3.4) requires an organisation to collect only that information necessary for the purposes that have been identified.

3**.2.3** The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.

3.2.4 When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. For an elaboration on consent, please refer to the Consent principle (Clause 3**.3).**

3.2.5 Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.

3.2.6 This principle is linked closely to the Limiting Collection principle (Clause 3.4) and the Limiting Use, Disclosure, and Retention principle (Clause 3.5).

3.3 Principle 3: Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organisations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organisation. In such cases, the organisation providing the list would be expected to obtain consent before disclosing personal information.

3.3.1 Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organisation will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organisation wants to use information for a purpose not previously identified).

3.3.2 The principle requires "knowledge and consent". Organisations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

3.3.3 An organisation shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified and legitimate purposes.

3.3.4 The form of the consent sought by the organisation may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organisations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a news magazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

3.3.5 In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organisation, in addition to using the individual's name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organisation can assume that the individual's request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.

3.3.6 The way in which an organisation seeks consent may vary, depending on the circumstances and the type of information collected. An organisation should generally seek express consent when the information is likely to be considered sensitive. Implied consent would

generally be appropriate when the information is less sensitive. Consent can also be given by an authorised representative (such as a legal guardian or a person having power of attorney).

3.3.7 Individuals can give consent in many ways. For example:

a) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;
b) a checkoff box may be used to allow individuals to request that their names and addresses not be given to other organisations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;
c) consent may be given orally when information is collected over the telephone; or
d) consent may be given at the time that individuals use a product or service.

3.3.8 An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organisation shall inform the individual of the implications of such withdrawal.

3.4 Principle 4: Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organisation. Information shall be collected by fair and lawful means.

3.4.1 Organisations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfill the purposes identified. Organisations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle (Clause 3.8).

3.4.2 The requirement that personal information be collected by fair and lawful means is intended to prevent organisations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.

3.4.3 This principle is linked closely to the Identifying Purposes principle (Clause 3.2) and the Consent principle (Clause 3**.3).**

3.5 Principle 5: Limiting Use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

3.5.1 Organisations using personal information for a new purpose shall document this purpose (see Clause 3.2.1).

3.5.2 Organisations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organisation may be subject to legislative requirements with respect to retention periods.

3.5.3 Personal information that is no longer required to fulfill the identified purposes should be destroyed, erased, or made anonymous. Organisations shall develop guidelines and implement procedures to govern the destruction of personal information.

3.5.4 This principle is closely linked to the Consent principle (Clause 3.3), the Identifying Purposes principle (Clause 3.2), and the Individual Access principle (Clause 3.9).

3.6 Principle 6: Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

3.6.1 The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.

3.6.2 An organisation shall not routinely update personal information, unless such a process is necessary to fulfill the purposes for which the information was collected.

3.6.3 Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.

3.7 Principle 7: Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

3.7.1 The security safeguards shall protect personal information against loss or theft, as well as unauthorised access, disclosure, copying, use, or modification. Organisations shall protect personal information regardless of the format in which it is held.

3.7.2 The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 3.3.1.

3.7.3 The methods of protection should include**:**

- physical measures, for example, locked filing cabinets and restricted access to offices;
- organisational measures, for example, security clearances and limiting access on a "need-to-know" basis; and
- technological measures, for example, the use of passwords and encryption.

3.7.4 Organisations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

3.7.5 Care shall be used in the disposal or destruction of personal information, to prevent unauthorised parties from gaining access to the information (see Clause 3.5.3).

3.8 Principle 8: Openness

An organisation shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

3.8.1 Organisations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organisation's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.

3.8.2 The information made available shall include:

- the name or title, and the address, of the person who is accountable for the organisation's policies and practices and to whom complaints or inquiries can be forwarded;
- the means of gaining access to personal information held by the organisation;
- a description of the type of personal information held by the organisation, including a general account of its use;
- a copy of any brochures or other information that explain the organisation's policies, standards, or codes; and
- what personal information is made available to related organisations (e.g., subsidiaries).

3.8.3 An organisation may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, an organisation may choose to make brochures available in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number.

3.9 Principle 9: Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Note: In certain situations, an organisation may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement should be limited and specific. The reasons for denying access should be provided to the individual upon request. Exceptions may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege.

3.9.1 Upon request, an organisation shall inform an individual whether or not the organisation holds personal information about the individual. Organisations are encouraged to indicate the source of this information. The organisation shall allow the individual access to this information. However, the organisation may choose to make sensitive medical information available through a medical practitioner. In addition, the organisation shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.

3.9.2 An individual may be required to provide sufficient information to permit an organisation to provide an account of the existence, use, and disclosure of personal information. The information provided shall only be used for this purpose.

3.9.3 In providing an account of third parties to which it has disclosed personal information about an individual, an organisation should attempt to be as specific as possible. When it is not possible to provide a list of the organisations to which it has actually disclosed information about an individual, the organisation shall provide a list of organisations to which it may have disclosed information about the individual.

3.9.4 An organisation shall respond to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organisation uses abbreviations or codes to record information, an explanation shall be provided.

3.9.5 When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organisation shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.

3.9.6 When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by the organisation. When appropriate, the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question.

3.10 Principle 10: Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organisation's compliance.

3.10.1 The individual accountable for an organisation's compliance is discussed in Clause 3.1.1.

3.10.2 Organisations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use.

3.10.3 Organisations shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. A range of these procedures may exist. For example, some regulatory bodies accept complaints about the personal-information handling practices of the companies they regulate.

3.10.4 An organisation shall investigate all complaints. If a complaint is found to be justified, the organisation shall take appropriate measures, including, if necessary, amending its policies and practices.

4.0 Other Principles Governing the Data Protection Policy and Data Protection Bill

Part I: General

1.1 Definitions

"Commissioner" means Data Commissioner;

"contact information" means information to enable a individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, and business email and fax number of the individual;

"data matching" means the comparison, whether manually or by means of any electronic or other device, of any record that contains personal information about individuals with other documents containing personal information about individuals for the purpose of producing new forms of information about the individuals;

"employee" includes a volunteer or service provider to a public authority;

"head of a public authority" means the Minister responsible for a ministry, a President or Chief Executive Officer of a corporation, the Chairman of an agency or counterpart, or such individual as designated by the Minister by order;

"health care body" means a regional health authority established under the Regional Health Authorities Act, 1994, a hospital, extended care facility, nursing home, clinic, mental health facility, and similar bodies as designated by the Minister by order but, for greater certainty, does not include the Ministry of Health;

"individual" means a natural person;

"information sharing agreement" means an agreement that sets conditions for one or more of the following: the exchange of personal information between a public authority and a person, a group or persons, or an organisation; the disclosure of personal information by a public authority to a person, a group of persons or an organisation; or a collection of personal information by a public authority from a person, a group of persons or an organisation;

"Minister" means the Minister to whom responsibility for data protection is assigned, and "Ministry" shall be construed accordingly;

"personal information" means information about an identifiable individual and includes employee personal information that does not include contact information or work product information;

"personal information bank" means a collection of personal information that is organised or retrievable by name of a individual or by an identifying number, symbol or other particular assigned to the individual;

"privacy impact assessment" means the assessment that is conducted to determine if a new enactment, system, project, programmeme or activity meets the requirements of the General Principles of Part I of this Policy or Bill;

"public authority" means Parliament, a Joint Select Committee of Parliament or a committee of either House of Parliament; the Court of Appeal, the High Court, the Industrial Court, the Tax Appeal Board or any court of summary jurisdiction; the Cabinet as constituted under the Constitution; a Ministry or a department or division of a Ministry; the Tobago House of Assembly, the Executive Council of the Tobago House of the Assembly or a division of the Tobago House of the Assembly; a municipal corporation established under the Municipal Corporations Act, 1990; a statutory body, responsibility for which is assigned to a Minister of Government; a company incorporated under the laws of Trinidad and Tobago that is owned or controlled by the State; a Service Commission established under the Constitution or other written law; or a body corporate or unincorporated that is established by the President's prerogative or by a Minister of Government in his official capacity or by another public authority; a body corporate or unincorporated entity in relation to any function that it exercises on behalf of the State, or which is supported, directly or indirectly, by Government funds and over which Government is in a position to exercise control; and any entity designated as a public authority by order of the Minister;

"record" means any document, correspondence, memorandum, book, plan, map, drawing, diagram, pictoral or graphic work, photograph, film, microform, sound recording, videotape, machine-readable record and any other documentary material, regardless of physical form or characteristics, and any copy of any of those things;

"sensory disability" means a disability that relates to sight or hearing;

"service provider" means a person retained under a contract to perform services for a public authority.

1.2 Bind the State

This Policy and Bill bind the State.

1.3 Exception

This Policy and Bill do not limit the information available by law to a party in a proceeding.

1.4 Same

This Policy and Bill do not affect the power of a court or a tribunal to compel a witness to testify or to compel the production of a document or other evidence.

1.5 Same

This Policy and Bill do not 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.

Part II: Principles Relating to Office and Powers of Data Commissioner

II.1 Appointment of Data Commissioner

1.1 The President, after consulting with the Prime Minister and the Leader of the Opposition, may appoint a Data Commissioner for a term of five years; the Data Commissioner may be re-appointed for a further term upon expiry of his term of office.

1.2 The President may appoint a Deputy Data Commissioner on similar terms.

1.3 The Commissioner and the Deputy Data Commissioner may not hold any other office or employment during their terms of office.

II.2 Resignation, removal or suspension of Commissioner

2.1 The Commissioner and the Deputy Data Commissioner may be removed from their offices only for cause, including physical or mental inability to fulfill the responsibilities of the office.

2.2 The Commissioner or Deputy Data Commissioner may resign from their offices by delivering a signed letter of resignation to the President.

II.3 Acting Commissioner

3.1 In the absence or incapacity of the Commissioner, the Deputy Data Commissioner may act in his place.

3.2 In the absence or incapacity of the Deputy Commissioner, the President may appoint an acting Commissioner.

II.4 Remuneration of the Commissioner

4.1 The Commissioner appointed under Principle 1.1 is entitled to be paid a salary equivalent to that paid to a Justice of the High Court of Trinidad and Tobago; the Deputy Data Commissioner shall be paid a proportionate amount.

4.2 The Commissioner, Deputy Data Commissioner and the staff of the Commissioner are entitled to be paid reasonable expenses incurred in the performance of their duties and functions.

II.5 Staff of Commissioner

5.1 The Commissioner may appoint, in accordance with the principles of appointments to the public service, employees necessary to enable the Commissioner to perform the duties of the office.

5.2 The Commissioner may retain any consultants, mediators or other persons necessary to enable the Commissioner to perform the duties of the office.

II.6 Delegation, with exception

6.1 With the exception of the matters set out in Principle 6.2, 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.

6.2 The Commissioner may delegate to only the Deputy Commissioner responsibilities regarding review of personal information that deals with matters that may be exempt from disclosure pursuant the *Freedom of Information Act, 1999*, sections 24-26 [documents dealing with cabinet confidences, defence and security, and international relations].

II.7 Duties of the Commissioner

7.1 The Commissioner has the following duties:

a) Promote the development of codes of conduct for guidance as to good practice;
b) Promote the following of good practices by persons subject to the Policy and the Bill;
c) Spread information about the Policy and the Bill;
d) Co-operate with counterparts in other jurisdictions to promote the protection of personal privacy in the public and private sectors;
e) Monitor compliance with the Policy and the Bill;
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) Publish guidelines regarding compliance with the Policy and Bill, 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;
h) Bring to the attention of the head of a public authority or organisation subject to a mandatory code of conduct any failure to meet the standards imposed by the Principles set out in Part I or the responsibilities established by Part III and Part IV of the Policy and Bill.
i) Issue public reports on the status of compliance with the Policy and Bill.

7.2 The Commissioner may accept such further functions and duties as may be assigned to him by the President by order, including but not limited to, the administration of the *Freedom of Information Act, 1999* and the Electronic Documents Policy and Bill.

II.8 General powers of Commissioner

The Commissioner is generally responsible for monitoring how the Policy and Bill are administered to ensure that their purposes are achieved and may:

a) conduct audits and investigations to ensure compliance with any provision of the Data Protection Policy or Bill or any other legislation or Policy for which he has been assigned responsibility;
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 organisation subject to a mandatory code of conduct, order the public authority to cease collection practices or destroy collections of personal information that contravene the Policy or the Bill;
d) authorise 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 organisation subject to the Policy or Bill;
f) authorise a public authority or an organisation subject to a mandatory code of conduct, upon the request of the head of the public authority or organisation, to 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 or organisation because of the repetitious or systematic nature of the requests or the requests are frivolous or vexatious;
g) authorise data matching by a public authority or public authorities;
h) make orders, including such terms and conditions as the Commissioner considers appropriate, following an appeal filed by an individual pursuant to Part III or Part IV of the Policy and Bill; and

i) make orders regarding compliance with the Principles of Part I by a public authority or an organisation subject to a mandatory code of conduct.

II.9 Orders of the Commissioner subject to judicial review

The orders and authorisations of the Commissioner may be reviewed by the High Court for errors of law or jurisdiction.

II.10 Powers of Commissioner in conducting an audit or inquiry of a public authority pursuant to Part III

10.1 Where the Commissioner is conducting an audit or inquiry into the practices of a public authority or determining an appeal pursuant to the Principles set out in Part III of this Policy or Bill, the Commissioner may:

a) require the production of any document or record that is in the custody or control of a public authority;
b) enter and inspect any premises occupied by a public authority for the purposes of an audit or inquiry;
c) summon and examine under oath any person who, in the Commissioner's opinion, may have information related to the inquiry and, for that purpose, the Commissioner may administer an oath.

10.2 The Commissioner shall not retain any information obtained from a record under Principle 10.1.

10.3 Before entering any premises of a public authority under Principle 10.1, the Commissioner shall notify the head of the public authority occupying the premises of his purpose.

10.4 The Commissioner may exercise his powers under this Principle with respect to Parliament, a Joint Select Committee of Parliament or a committee of either House of Parliament; 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 the Assembly or a division of the Tobago House of the Assembly only with the consent of the Speaker of the House and Senate, the Chief Justice, or the Head of the Executive Council, as the case may be.

II.11 Power of Commissioner to conduct audit or inquiry pursuant to Part IV

11.1 Where the Commissioner is conducting an audit or inquiry into the compliance practices of a person subject to the provisions of an enforceable code of conduct pursuant to Part IV of this Policy or Bill, the Commissioner may, pursuant to the authority provided by a warrant of a court:

d) require the production of any document or record that is in the custody or control of a person subject to the enforceable code of conduct ;
e) enter and inspect any premises occupied by a person subject to an enforceable code of conduct for the purposes of an audit or inquiry;
f) summon and examine under oath any person who, in the Commissioner's opinion, may have information related to the inquiry and, for that purpose, the Commissioner may administer an oath.

11.2 The Commissioner shall not retain any information obtained from a record under Principle 11.1.

II.12 Statements made to Commissioner not admissible

A statement made or an answer given by a person during an investigation or inquiry by the Commissioner is inadmissible in evidence in court or any other proceeding, except

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

II.13 Protection against libel or slander actions

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

II.14 Restrictions on disclosure of information by Commissioner and staff

The Commissioner and anyone acting for or under the direction of the Commissioner must not disclose any information obtained in performing their duties, powers and functions under this Policy or Bill, excepted as provided below:

a) The Commissioner may disclose, or may authorise anyone acting for or under the direction of the Commissioner to disclose, information that is necessary to conduct an investigation, audit or inquiry under this Policy or Bill or establish grounds for findings and recommendations contained in a report under the Policy or Bill.
b) The Commissioner may disclose, or may authorise anyone acting for or under the direction of the Commissioner to disclose, information in the course of a prosecution or an appeal from or judicial review of a decision of the Commissioner.

II.15 Protection of Commissioner and staff

No proceedings lie against the Commissioner or against 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 performed in good faith.

II.16 Whistle-blowing protection

An employer, whether or not a public authority, must not dismiss, suspend, demote, discipline, harass or otherwise disadvantage an employee or the employer or deny that employee a benefit, because

a) The employee, acting in good faith and on the basis of reasonable belief has notified the Commissioner that the employer or any other person has contravened or is about to contravene this Policy or Bill;
b) The employee, acting in good faith and on the basis of reasonable belief has done or stated the intention of doing anything that is required to be done in order to avoid having any person contravene this Policy or Bill;
c) The employee, acting in good faith and on the basis of reasonable belief has refused to do or stated the intention of refusing to do anything that is in contravention of this Policy or Bill;
d) The employer believes that the employee will do anything described in paragraph a), b), c) or d).

II.17 Annual report of Commissioner

17.1 The Commissioner shall make a report annually to Parliament on the activities of his Office during the previous year.

17.2 The Commissioner may make a special report to Parliament at any time commenting on any matters within the scope, duties and functions of the Commissioner and the matter is of such

urgency or importance that it should not be deferred to the time of the next annual report to Parliament.

Part III: Principles for Protection of Personal Data by Public Authorities

III.1 Limitations on the definition of "personal information"

1.1 The following information about a individual who is or has been an employee or official of a public authority is not personal information for the purposes of the Policy or Bill:

a) The fact that the individual is or was an official or employee of the public authority;
b) The title, business address and telephone number of the individual;
c) The classification, salary range and responsibilities of the position held by the individual;
d) The name of the individual on a document prepared by the individual in the course of employment;
e) The personal opinions or views of the individual given in the course of employment.

III.2 Same

Information about a individual who is or was performing services under contract for a public authority that relates to the services performed, including the terms of the contract, the name of the individual, and the opinions or views of the individual given in the course of the performance of those services is not personal information for the purposes of the Policy or Bill.

III.3 Same

Information relating to any discretionary benefit of a financial nature, including the granting of a licence or permit, conferred on a individual, including the name of the individual and the exact nature of the benefit is not personal information for the purposes of the Policy or the Bill.

III.4 Same

Information about an individual who has been dead for more than twenty years is not personal information for the purposes of this Policy or Bill.

III.5 Does not apply to health care bodies

This Part of the Policy or Bill does not apply to health care bodies.

III.6 Collection of personal information

No personal information may be collected by or for a public authority unless

a) The collection of that information is expressly authorized by or under an Act,
b) That information is collected for the purposes of law enforcement, or
c) That information relates directly to and is necessary fro an operating programme or activity of the public authority.

III.7 Personal information to be collected directly

A public authority must collect personal information or cause personal information to be collected directly from the individual the information is about unless

a) Another method of collection is authorized by the individual, by the Commissioner or by another enactment;
b) The collection of information is necessary for the medical treatment of a 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;
c) The information is collected for the purpose of
    i) determining the suitability for an honour or award including an honourary degree, scholarship, prize or bursary;
    ii) proceeding before a court or a judicial or quasi-judicial tribunal;
    iii) collecting a debt or fine or making a payment or

iv) law enforcement.

III.8 Individual to be informed of purpose

A public authority must ensure that the individual from whom it collects personal information or causes personal information to be collected is told

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.

III.9 Exception

Principle III.8 does not apply

a) if compliance with Principle III.8 would result in the collection of inaccurate information;
b) if compliance with Principle III.8 it would defeat the purpose or prejudice the use for which the information is to be collected; or
c) if compliance with Principle III.8 would
   i) harm a law enforcement matter,
   ii) 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,
   iii) harm the effectiveness of investigative techniques and procedures currently used, or likely to be used, in law enforcement,
   iv) reveal the identity of a confidential source of law enforcement information,
   v) reveal criminal intelligence that has a reasonable connection with the detection, prevention or suppression or organised criminal activities or of serious and repetitive criminal activities,
   vi) endanger the life or physical safety of a law enforcement officer or any other individual,
   vii) reveal any information relating to or used in the exercise of prosecutorial discretion,
   viii) deprive a person of the right to a fair trial or impartial adjudication,
   ix) reveal a record that has been confiscated from a person by a peace office in accordance with an enactment,
   x) facilitate the escape from custody of an individual who is sunder lawful detention,
   xi) facilitate the commission of an offence under an enactment of Trinidad and Tobago, or harm the security of ay property or system, including a building, a vehicle, a computer system or a communications system.

III.10 Retention of personal information used for an administrative purpose

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 is has been used as may be prescribed by order of the Minister in order to ensure that the individual to whom it relates has a reasonable opportunity to obtain access to that information.

III.11 Accuracy of personal information

If a individual's personal information 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 must make every reasonable effort to ensure that the personal information is accurate and complete.

III.12 Protection of personal information
A public authority must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, alternation, disclosure or disposal.

III.13 Storage and access in Trinidad and Tobago
A public authority must 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 one of the following applies:

a) if the individual the information is about has identified the information and has consented in the prescribed manner to its being stored in or accessed from another jurisdiction;
b) if it is stored in or accessed from another jurisdiction for the purposes of disclosure allowed under this Policy or Bill.

III.14 Disposal of personal information
A public authority shall dispose of the personal information in its control or custody in accordance with regulations established by order of the Minister.

III.15 Use of personal information
Personal information under the 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 disclosed by the public authority pursuant to Principle III.18.

III.16 Consistent Purpose
A 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 authorised programmeme of, a public authority that uses or discloses the information or causes the information to be used or disclosed

III.17 Disclosure of personal information
Personal information under the control of a public authority shall not, be disclosed by the public authority without the consent of the individual to whom it relates, except in accordance with Principle III.18, III.19 or III.20.

III.18 When personal information may be disclosed
Subject to any other Act of Parliament, personal information under the control of a public authority may 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 Act of Parliament or any order made pursuant to such an Act that authorises its 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 any law of Trinidad and Tobago 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 within Trinidad and Tobago to another law enforcement agency within Trinidad and Tobago for the purpose of enforcement of the laws of Trinidad and Tobago;
g) to a law enforcement agency in a foreign country under an arrangement, a written agreement, a treaty, or under the authority of the Government of Trinidad and Tobago;
h) if the head of a public authority agrees that a compelling circumstances that affect anyone's health or safety and if notice of the disclosure is mailed to the last known address of the individual the information is about, unless the head of the public authority has a reasonable belief that providing notification could harm someone's health or safety;
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 to a public authority or making a payment owing by the government of Trinidad and Tobago or by a public authority to an individual.

III.19 Disclosure for research or statistical purposes

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 the research,
c) any record linkage is not harmful to the individuals 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 of 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 Policy and Bill and any of the public authority's policies and procedures relating to the confidentiality of personal information.

III.20 Disclosure for archival or historical purposes

The archives of the Government of Trinidad and Tobago or the archives of a public authority may disclosed 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 personal privacy,
b) the disclosure is for historical research and is in accordance with Principle III.18,
c) the information is about someone who has been dead for 20 or more years, or
d) the information is in a record that has been in existence for 100 or more years.

III. 21 Privacy impact assessment and mitigation

21.1 Every Ministry of the Government of Trinidad and Tobago must prepare a privacy impact assessment of any new enactment, system, project, programmeme or activity.

21.2 Having prepared a privacy impact assessment, every Ministry of the Government of Trinidad and Tobago shall take all reasonable steps to avoid unnecessary intrusions into personal privacy

when designing, implementing or enforcing enactments, systems, projects, programmemes or activities.

III.22 Personal information banks

The head of a public authority shall cause to be included in personal information banks all personal information under the control or in the custody of the public authority that

a) has been used, is being used or is available for the use for an administrative purpose; or
b) is organised or intended to be retrieved by the name of an individual or by an identifying number, symbol or other particular assigned to an individual.

III.23 Exception

Principle III.22 does not apply to personal information under the custody or control of the Archives of Trinidad and Tobago that has been transferred there by a public authority for historical or archival purposes.

III.24 Information sharing

24.1 Where a public authority intends to share information with another public authority, it shall do so only pursuant to an agreement in a form approved by the Commissioner.

25. Data matching must be approved by Commissioner

25.1 Before a public authority may match personal information from a record with personal information from another record, whether or not pursuant to an information sharing agreement, the public authority shall obtain the authorization of the Commissioner.

25.2 In determining whether to authorise data matching by a public authority or public authorities, the Commissioner shall consider:

a) whether or not the objective of the matching programmeme relates to a matter of significant public importance;
b) whether or not the matching programmeme would achieve that objective in a way that would achieve monetary savings that are both significant and quantifiable or will achieve other significant benefits to society;
c) whether or not the public interest in allowing the matching programme to proceed outweighs the public interest in adhering to the information privacy principles set out in Part I that the programmeme would otherwise contravene;
d) whether or not the programmeme involves information matching on a scale that is excessive, having regard to the number of public authorities that will be involved in the programmeme and the amount of detail about an individual that will be matched under the programmeme.

25.3 In approving data matching by a public authority or public authorities, the Commissioner may impose whatever terms and conditions he considers appropriate.

III. 26 Personal information index

The Minister shall publish periodically, but no less than annually, an index of the personal information that is held by public authorities that includes a summary of the following:

a) the personal information banks that are in the custody or control of each public authority;
b) the information sharing agreements entered into by any public authority with another public authority or other person;
c) the data matching activities approved by the Commissioner;
d) the contact information of the official to whom requests relating to personal information contained in the data bank should be sent;

e) a statement of the purposes for which personal information in the data bank was obtained or compiled and a statement of the uses consistent with those purposes for which the information is used or disclosed;
f) a statement of the retention and disposal standards and practices that apply to the personal information in the data bank;
g) privacy impact assessments prepared by any Ministry of the Government of Trinidad and Tobago.

III. 27 Right of access to personal information

27.1 Every individual who is a citizen of or is 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 or 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.

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

27.3 Where a head of a public authority provides personal information in accordance with the provisions of this Policy or Bill, the head may provide the information in response to an oral request, in appropriate circumstances.

III.28 Refusal of access to personal information

A head of a public authority may refuse to disclose personal information to the individual to whom the information relates,

a) where the disclosure would constitute an unjustified invasion of another individual's personal privacy;
b) where it is medical information where the disclosure could reasonably be expected to prejudice the mental or physical health of the individual;
c) where it is a correctional record where the disclosure could reasonably be expected to reveal information supplied in confidence;
d) where 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;
e) where a disclosure would result in disclosure of information that is exempt from disclosure under Part IV of the *Freedom of Information Act, 1999*.

III. 29 Severance and refusal to disclose existence of information

29.1 A head of a public authority shall make every effort to sever information that is exempt from disclosure pursuant to Principle III.28 from information that may be made available to the individual requesting access to his or her personal information and make the non-exempt information available.

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

III.30 Request for personal information under the Access to Information Act, 1999

Where an individual makes a request for his or her own personal information under the *Access to Information Act, 1999*, that request shall be treated as a request under this Policy or Bill.

III.31 Exercise of rights of deceased, etc. persons

Any right or power conferred on an individual by the Policy or Bill may be exercised

a) where the individual is deceased, by the individual's personal representative if the exercise of the right or power relates to the administration of the individual's estate;
b) by the individual's attorney under a power of attorney or the individual's guardian or the person or of property;
c) where the individual is less than 18 years of age, by a person who has lawful custody of the individual.

III.32 Responsibilities of public authorities

32.1 Where a request is made for access to personal information pursuant to Principle III.28 or Principle III.30, the head of the public authority shall, within thirty days after the request is received,

a) where access is granted in whole or in part, give the information to the individual who made the request, or
b) where access is refused in whole or in part, give the individual who made the request a written response stating:

    i) that the information does not exist; or
    ii) the specific provision of the Policy or Bill on which a refusal could reasonably be expected to be based if the information existed;

c) where the access is refused in whole or in part, give the individual who made the request information regarding the right to appeal to the Commissioner.

32.2 Where access is granted in whole or in part, the head of the public authority shall ensure that the information is available in a comprehensible form, including where reasonable, comprehensible to an individual with a sensory disability.

III.33 Right to request correction of personal information

33.1 Where an individual believes there is an error or omission in his or her personal information, the individual may request the head of the public authority that has the information in its custody or under its control to correct the information.

33.2 If no correction is made in response to a request under Principle 33.1, the head of the public authority must annotate the information with the correction that was requested but not made.

33.3 On correcting or annotating personal information under this principle, the head of a public authority must notify any other public authority or any third party to whom that information has been disclosed during the one-year period before the correction was requested.

33.4 Upon being notified under Principle 33.3 of a correction or annotation of personal information, a public authority must make the correction or annotation on any record of that information in its custody or control.

III.34 Appeal to the Data Commissioner

Any individual who has filed a request for his or her personal information pursuant to Principles III.28 or III.30 of this Policy or Bill or who has requested correction of personal information pursuant to Principle III.33 of this Policy or Bill may appeal any decision of the head of the public authority under this Policy or Bill to the Data Commissioner.

III.35 Time For Application

An appeal to the Commissioner must be made within thirty days after the notice was given of the decision appealed from by filing with the Commissioner written notice of appeal.

III.36 Immediate dismissal

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.

III.37 Notice of application for appeal

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.

III. 38 Mediation

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

III.39 Inquiry

The Commissioner may conduct an inquiry to review the head's decision if:

the Commissioner has not authorised a mediator to conduct an investigation under Principle 36; or

the Commissioner has authorised a mediator to conduct an investigation under Principle 36, but no settlement has been reached.

III.40 Inquiry in private

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

III.41 Representations

The individual who requested access to personal information, the head of the public authority concerned and any affected party shall be given an opportunity make representations to the Commissioner, but none is entitled to be present during, to have access to, or to comment on representations made to the Commissioner by any other person.

III.42 Right to counsel

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

III.43 Burden of proof

Where the head of a public authority refuses access to personal information, the burden of proof on the balance of probabilities that the information lies within one of the specified exemptions of the Policy or Bill lies upon the head of the public authority.

Part IV: Principles for Protection of Personal Data by the Private Sector

IV.1 General Privacy Principles are good practice

1.1 Any person who collects, retains, manages, uses, processes, or stores personal information in Trinidad and Tobago, or who collects personal information from individuals in Trinidad and Tobago, or who uses an intermediary or internet service provider located in Trinidad and Tobago should endeavour to follow the General Privacy Principles set out in Part I as examples of good practice in dealing with personal information.

IV.2 Codes of Practice

The Commissioner shall work with industry, industry groups and persons 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 complaint 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 appear to the Commissioner to be appropriate.

IV. 3 Commissioner may require development of code of conduct

3.1 Where, in the opinion of the Commissioner, the public interest warrants the 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 by order may require the development of a code of conduct and set a time limit for its development.

3.2 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.

IV. 4 Approval of a code of conduct

4.1 The Commissioner may approve a code of conduct dealing with compliance with the Principles set out in Part I developed by an industry sector, an industry organisation, a professional body or any other person who comes forward to the Commissioner with an application for approval of a code.

4.2 In determining whether to approve a code of conduct, the Commissioner shall consider:

a) compliance with the Principles set out in Part I;
b) use and adequacy of dispute resolution mechanisms within the industry, as well as within individual firms;
c) potential for development or encouragement of anti-competitive conduct;
d) adequacy of the process used to develop the code of conduct, including involvement of stakeholders, such as relevant consumers, suppliers, and other interested groups;
e) role of industry sector regulators, if any;
f) any other matters that the Commissioner considers relevant.

IV. 5. Mandatory codes of conduct

5.1 Where the Commissioner has approved a code of conduct, the Minister may by order make the code legally enforceable with respect to those to whom the code applies as a regulation pursuant to the Bill.

5.2 An order of the Minister making a code legally enforceable pursuant to Principle 4.3 shall be placed before Parliament and may be subject to a negative resolution of the House.

5.3 In the alternative, where a government regulator has the jurisdiction over an industry, economic sector or activity so that the code of conduct dealing with the application of the General Privacy Principles can be made mandatory pursuant to other legislation, the regulator may make a code of conduct approved by the Commissioner mandatory.

5.4 Where an industry regulator has mandated compliance with a code of conduct dealing with the protection of personal privacy that has been approved by the Commissioner and the legislation under which the code of conduct has been made mandatory has adequate provisions for complaint resolution and sanctions for non-compliance with the provisions of the code of conduct, the Commissioner may forebear from exercising his powers with respect to compliance.

IV. 6 Complaint to the Commissioner

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

a) where the individual has asked the organisation for access to or the correction of personal information, ask the Commissioner to conduct a review of the resulting decision, act or failure to act of the organisation; or
b) make a complaint to the Commissioner regarding an alleged failure of the organisation to comply with the provisions of the mandatory code of conduct.

IV. 7 Application of provisions of Part III

Principles III.36 to III.43 apply to a request or complaint made to the Commissioner pursuant to Principle IV.6.

Part V: Offences

V.1 Obstruction

Any person who willfully obstructs the Data Commissioner or any person acting for or under the direction of the Commissioner in the course of carrying out an audit or an investigation is guilty of an offence.

V.2 False and misleading statements

2.1 Any person who makes a request for access to or correction of personal information under false pretenses is guilty of an offence.

2.2 Any person who willfully makes a false statement to, misleads, or attempts to mislead the Commissioner in the performance of his or her functions under this Policy or Bill is guilty of an offence.

V.3 Failure to comply with an order

Any person who fails to comply with an order of the Commissioner is guilty of an offence.

V.4 Violation of whistle-blowing provisions

Every person who contravenes the provisions of Principle II.11.16 is guilty of an offence.

V.5 Contravention of Policy or Bill

5.1 Every person who willfully discloses personal information in contravention of this Bill is guilty of an offence.

5.2 Every person who willfully maintains a personal information bank that contravenes this Bill is guilty of an offence.

V.6 Breach of obligations of confidentiality

Every person who breaches the confidentiality obligations established by Principle II.11.14 is guilty of an offence.

V.7 Directors and officers

Where a corporation commits an offence under this Act, any officer, director or agent of the corporation who directed, authorized, assented to, acquiesced in or participated in the commission of an offence is a party to and guilty of the offence, and is liable to the punishment provided for the offence, whether or not the corporation has been prosecuted and convicted.

V.8 Duties of directors

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

a) this Act and the regulations; and
b) any orders imposed by the Commissioner or his delegate.

V.9 Penalties

Every person who is guilty of an offence under this Act is liable

a) upon indictment, to a fine of not more than XX or to imprisonment for a term of not more than XX years, or both if a individual or a fine of XXXX if a corporation; and
b) upon summary conviction, to a fine of not more than YY or to imprisonment for a term of not more than YY years or both if a individual or a fine of YYYY if a corporation.

Bibliography

1) British Columbia, Canada, Personal Information Protection Act, 2003, Chapter 63
2) British Columbia, Canada, Freedom of Information and Protection of Privacy Act. R.S.B.C. 1996, Chapter 165.
3) Canada, the Personal Information and Protection of Electronic Documents Act, S.C. 2000, Chapter 5.
4) Canada, Privacy Act, S.C.
5) Ontario, Canada, Freedom of Information and Protection of Privacy Act, R.S.O., 1990, Chapter F. 31.
6) European Community, 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 free movement of such data.
7) Organisation for Economic Co-operation and Development, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/dsti/sti/it/secur/index.htm>
8) Perrin, Stephanie et al., The Personal Information and Electronic Documents Act: An Annotated Guide (Toronto, Irwin Law, 2001).
9) New Zealand, Privacy Act, 1993
10) Australia, Office of the Federal Privacy Commissioner, Guidelines on Privacy Code Development, September 2001.
11) United Nations Conference on Trade and Development, 'E-Commerce and Development Report 2004', UNCTAD Secretariat, United Nations New York and Geneva
12) UK White Paper, 'Computers and Privacy' (Cmnd 6353), 1975.
13) Levine, S., 'Provincial Approaches to Regulating Health Care Privacy, An Overview', Fasken Martineau Du Moulin LLP, Toronto, 2002.
14) Davino, M. 'Assessing Privacy Risk in Outsourcing' *Journal of AHIMA* 75, no.3 (March 2004): 42-46.
15) 'Law and Technology Workshop for the Caribbean', Commonwealth Secretariat, 2004, Available online http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7B7D3F51D4-02A1-42FE-A8B5-7CE08D36DDF0%7D_LawTechnologyFullReport2003.pdf (Last Accessed December 2004)
16) 'Data Protection Regulation in India', Financial Times 2004, Available online http://www.fdimagazine.com/news/fullstory.php/aid/711/Data_protection_regulations_in_India.html (Last Accessed December 2004)
17) Radwasnski, G., Privacy Commissioner of Canada, 'The Spanish Data Protection Authority and Latin-American Centre of Data Protection Conference', 2002, Office of the Privacy Commissioner of Canada, Available online http://www.privcom.gc.ca/speech/02_05_a_020520_e.asp (Last Accessed December 2004)
18) Rotenberg, M., Lauran, C., 'Privacy and Human Rights 2004 – An International Survey of Privacy Laws and Developments', Privacy International