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

Privacy and Data Protection: Model Policy Guidelines & Legislative Texts

HIPCAR

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

European Commission

CARICOM

CTU

ITU

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

Privacy and Data Protection:

Model Policy Guidelines & Legislative Texts

HIPCAR

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

Foreword

Information and communication technologies (ICTs) are shaping the process of globalisation. Recognising their potential to accelerate the Caribbean region's economic integration and thereby its greater prosperity and social transformation, the Caribbean Community (CARICOM) Single Market and Economy has developed an ICT strategy focusing on strengthened connectivity and development.

Liberalisation of the telecommunication sector is one of the key elements of this strategy. Coordination across the region is essential if the policies, legislation, and practices resulting from each country's liberalisation are not to be so various as to constitute an impediment to the development of a regional market.

The project 'Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures' (HIPCAR) has sought to address this potential impediment by bringing together and accompanying all 15 Caribbean countries in the Group of African, Caribbean and Pacific States (ACP) as they formulate and adopt harmonised ICT policies, legislation, and regulatory frameworks. Executed by the International Telecommunication Union (ITU), the project has been undertaken in close cooperation with the Caribbean Telecommunications Union (CTU), which is the chair of the HIPCAR Steering Committee. A global steering committee composed of the representatives of the ACP Secretariat and the Development and Cooperation - EuropeAid (DEVCO, European Commission) oversees the overall implementation of the project.

This project is taking place within the framework of the ACP Information and Telecommunication Technologies (@CP-ICT) programme and is funded under the 9th European Development Fund (EDF), which is the main instrument for providing European aid for development cooperation in the ACP States, and co-financed by the ITU. The @CP-ICT aims to support ACP governments and institutions in the harmonization of their ICT policies in the sector by providing high-quality, globally-benchmarked but locally-relevant policy advice, training and related capacity building.

All projects that bring together multiple stakeholders face the dual challenge of creating a sense of shared ownership and ensuring optimum outcomes for all parties. HIPCAR has given special consideration to this issue from the very beginning of the project in December 2008. Having agreed upon shared priorities, stakeholder working groups were set up to address them. The specific needs of the region were then identified and likewise potentially successful regional practices, which were then benchmarked against practices and standards established elsewhere.

These detailed assessments, which reflect country-specific particularities, served as the basis for the model policies and legislative texts that offer the prospect of a legislative landscape for which the whole region can be proud. The project is certain to become an example for other regions to follow as they too seek to harness the catalytic force of ICTs to accelerate economic integration and social and economic development.

I take this opportunity to thank the European Commission and ACP Secretariat for their financial contribution. I also thank the Caribbean Community (CARICOM) Secretariat and the Caribbean Telecommunication Union (CTU) Secretariat for their contribution to this work. Without political will on the part of beneficiary countries, not much would have been achieved. For that, I express my profound thanks to all the ACP governments for their political will which has made this project a resounding success.

Brahima Sanou
BDT, Director

Acknowledgements

The present document represents an achievement of the regional activities carried out under the HIPCAR project "Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures", officially launched in Grenada in December 2008.

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

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

The HIPCAR Steering Committee – chaired by the Caribbean Telecommunications Union (CTU) – provided guidance and support to a team of consultants, including Ms. Karen Stephen-Dalton and Mr. Kwesi Prescod. The draft document was then reviewed, discussed and adopted by broad consensus by participants at two consultation workshops for the HIPCAR Working Group on Information Society Issues, held in Saint Lucia on 8-12 March 2010 and in Saint Kitts and Nevis on 19 – 22 July 2010 (see Annexes). The explanatory notes to the model legislative text in this document were prepared by Mr. Prescod addressing, *inter alia*, the points raised at the second workshop.

ITU would like to especially thank the workshop delegates from the Caribbean ICT and telecommunications ministries, representatives from the ministries of justice and legal affairs and other public sector bodies, regulators, academia, civil society, operators, and regional organisations, for their hard work and commitment in producing the contents of this report. This broad base of public sector participation representing different sectors allowed the project to benefit from a cross-section of views and interests. The contributions from the Caribbean Community (CARICOM) Secretariat and the Caribbean Telecommunications Union (CTU) are also gratefully acknowledged.

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

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

Table of contents

Introduction

1.1. HIPCAR Project – Aims and Beneficiaries

The HIPCAR project[1] was officially launched in the Caribbean by the International Telecommunication Union (ITU) and the European Union (EU) in December 2008, in close collaboration with the Caribbean Community (CARICOM) Secretariat and the Caribbean Telecommunications Union (CTU). The HIPCAR Project is part of a global ITU-EC-ACP project encompassing also in sub-Saharan Africa and the Pacific.

HIPCAR's objective is to assist CARIFORUM[2] countries in the Caribbean to harmonize their information and communication technology (ICT) policies, legislation and regulatory procedures so as to create an enabling environment for ICT development and connectivity, thus facilitating market integration, fostering investment in improved ICT capabilities and services, and enhancing the protection of ICT consumers' interests across the region. The project's ultimate aim is to enhance competitiveness and socio-economic and cultural development in the Caribbean region through ICTs.

In accordance with Article 67 of the Revised Treaty of Chaguaramas, HIPCAR can be seen as an integral part of the region's efforts to develop the CARICOM Single Market & Economy (CSME) through the progressive liberalization of its ICT services sector. The project also supports the CARICOM Connectivity Agenda and the region's commitments to the World Summit on the Information Society (WSIS), the World Trade Organization's General Agreement on Trade in Services (WTO-GATS) and the Millennium Development Goals (MDGs). It also relates directly to promoting competitiveness and enhanced access to services in the context of treaty commitments such as the CARIFORUM states' Economic Partnership Agreement with the European Union (EU-EPA).

The beneficiary countries of the HIPCAR project include Antigua and Barbuda, The Bahamas, Barbados, Belize, The Commonwealth of Dominica, the Dominican Republic, Grenada, Guyana, Haiti, Jamaica, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Suriname, and Trinidad and Tobago.

1.2. Project Steering Committee and Working Groups

HIPCAR has established a project Steering Committee to provide it with the necessary guidance and oversight. Members of the Steering Committee include representatives of Caribbean Community (CARICOM) Secretariat, Caribbean Telecommunications Union (CTU), Eastern Caribbean Telecommunications Authority (ECTEL), Caribbean Association of National Telecommunication Organisations (CANTO), Caribbean ICT Virtual Community (CIVIC), and International Telecommunication Union (ITU).

In order to ensure stakeholder input and relevance to each country, HIPCAR Working Groups have also been established with members designated by the country governments – including specialists from ICT agencies, justice and legal affairs and other public sector bodies, national regulators, country ICT focal

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

2 The CARIFORUM is a regional organisation of fifteen independent countries in the Caribbean region (Antigua and Barbuda, Bahamas, Barbados, Belize, Dominica, Dominican Republic, Grenada, Guyana, Haiti, Jamaica, Saint Christopher and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Suriname, and Trinidad and Tobago). These states are all signatories to the ACP–EC Conventions.

points and persons responsible for developing national legislation. This broad base of public sector participation representing different sectors allowed the project to benefit from a cross-section of views and interests. The Working Groups also include representatives from relevant regional bodies (CARICOM Secretariat, CTU, ECTEL and CANTO) and observers from other interested entities in the region (e.g. civil society, the private sector, operators, academia, etc.).

The Working Groups have been responsible for covering the following two work areas:

1. *ICT Policy and Legislative Framework on Information Society Issues*, dealing with six sub-areas: e-commerce (transactions and evidence), privacy & data protection, interception of communications, cybercrime, and access to public information (freedom of information).
2. *ICT Policy and Legislative Framework on Telecommunications*, dealing with three sub-areas: universal access/service, interconnection, and licensing in a convergent environment.

The reports of the Working Groups published in this series of documents are structured around these two main work areas.

1.3. Project Implementation and Content

The project's activities were initiated through a Project Launch Roundtable organized in Grenada, on 15-16 December 2008. To date, all of the HIPCAR beneficiary countries – with the exception Haiti – along with the project's partner regional organizations, regulators, operators, academia, and civil society have participated actively in HIPCAR events including – in addition to the project launch in Grenada – regional workshops in Trinidad & Tobago, St. Lucia, St. Kitts and Nevis, Suriname and Barbados.

The project's substantive activities are being led by teams of regional and international experts working in collaboration with the Working Group members, focusing on the two work areas mentioned above.

During *Stage I* of the project – just completed – HIPCAR has:

1. Undertaken assessments of the existing legislation of beneficiary countries as compared to international best practice and in the context of harmonization across the region; and
2. Drawn up model policy guidelines and model legislative texts in the above work areas, from which national ICT policies and national ICT legislation/regulations can be developed.

It is intended that these proposals shall be validated or endorsed by CARICOM/CTU and country authorities in the region as a basis for the next phase of the project.

Stage II of the HIPCAR project aims to provide interested beneficiary countries with assistance in transposing the above models into national ICT policies and legislation tailored to their specific requirements, circumstances and priorities. HIPCAR has set aside funds to be able to respond to these countries' requests for technical assistance – including capacity building – required for this purpose.

1.4. Overview of the Six HIPCAR Model Policy Guidelines and Legislative Texts Dealing with Information Society Issues

Countries worldwide as well as in the Caribbean are looking for ways to develop legal frameworks addressing the needs of information societies with a view to leveraging the growing ubiquity of the World Wide Web as a channel for service delivery, ensuring a safe environment and the processing power of information systems to increase business efficiency and effectiveness.

The Information Society is based on the premise of access to information and services and utilizing automated processing systems to enhance service delivery to markets and persons *anywhere in the world*. For both users and businesses the information society in general and the availability of information and communication technology (ICT) offers unique opportunities. As the core imperatives of commerce remain unchanged, the ready transmission of this commercial information creates opportunities for enhanced business relationships. This ease of exchange of commercial information introduces new paradigms: firstly, where information is used to support transactions related to physical goods and traditional services; and secondly, where information itself is the key commodity traded.

The availability of ICTs and new network-based services offer a number of advantages for society in general, especially for developing countries. ICT applications, such as e-Government, e-Commerce, e-Education, e-Health and e-Environment, are seen as enablers for development, as they provide an efficient channel to deliver a wide range of basic services in remote and rural areas. ICT applications can facilitate the achievement of millennium development targets, reducing poverty and improving health and environmental conditions in developing countries. Unhindered access to information can support democracy, as the flow of information is taken out of the control of state authorities (as has happened, for example, in Eastern Europe). Given the right approach, context and implementation processes, investments in ICT applications and tools can result in productivity and quality improvements.

However, the transformation process is going along with challenges as the existing legal framework does not necessary cover the specific demands of a rapidly changing technical environment. In cases where information supports trade in traditional goods and services, there needs to be clarity in how traditional commercial assumptions are effected; and in the instance where information is the commodity traded, there needs to be protection of the creator/ owner of the commodity. In both instances, there needs to be rationalization of how malfeasance is detected, prosecuted and concluded in a reality of trans-border transactions based on an intangible product.

The Six Inter-related Model Frameworks

The HIPCAR project has developed six (6) inter-related model frameworks that provide a comprehensive legal framework to address the above mentioned changing environment of information societies by guiding and supporting the establishment of harmonized legislation in the HIPCAR beneficiary countries.

Firstly a legal framework was developed to protect the right of users in a changing environment and thereby among other aspects ensuring consumer and investor confidence in regulatory certainty and protection of privacy, HIPCAR model legislative texts were developed to deal with considerations relating to: **Access to Public Information (Freedom of Information)** – geared to encouraging the appropriate culture of transparency in regulatory affairs to the benefit of all stakeholders; and **Privacy and Data Protection** – aimed at ensuring the protection of privacy and personal information to the satisfaction of the individual. This latter framework is focused on appropriate confidentiality practices within both the public and private sectors.

Secondly, in order to facilitate harmonization of laws with regard to the default expectations and legal validity of contract-formation practices, a HIPCAR model legislative text for **Electronic Commerce (Transactions)**, including electronic signatures was developed. This framework is geared to provide for the equivalence of paper and electronic documents and contracts and for the foundation of undertaking commerce in cyber-space. A legislative text dealing with **Electronic Commerce (Evidence)** – the companion to the Electronic Commerce (Transactions) framework, was added to regulate legal evidence in both civil and criminal proceedings.

To ensure that grave violations of the confidentiality, integrity and availability of ICT and data can be investigated by law enforcement, model legislative texts were developed to harmonise legislation in the field of criminal law and criminal procedural law. The legislative text on **Cybercrime** defines offences, investigation instruments and the criminal liability of key actors. A legislative text dealing with the **Interception of Electronic Communications** establishes an appropriate framework that prohibits the illegal interception of communication and defines a narrow window that enables law enforcement to lawfully intercept of communication if certain clearly defined conditions are fulfilled.

Developing the Model Legislative Texts

The model legislative texts were developed by taking into account key elements of international trends as well as legal traditions and best practices from the region. This process was undertaken to ensure that to the frameworks optimally meet the realities and requirements of the region of HIPCAR beneficiary countries for which and by which they have been developed. Accordingly, the process involved significant interaction with stakeholders at each stage of development.

The first step in this complex process was an assessment of existing legal frameworks within the region through a review of the laws related to all relevant areas.. In addition to enacted legislation, the review included, where relevant, bills which had been prepared but had yet to complete the process of promulgation. In a second step, international best practices (for example from United Nations, OECD, EU, the Commonwealth, UNCITRAL and CARICOM) as well as advanced national legislation (for example from the UK, Australia, Malta and Brazil, among others) were identified. Those best practices were used as benchmarks.

For each of the six areas, complex legal analyses were drafted that compared the existing legislation in the region with these benchmarks. This comparative law analysis provided a snapshot of the level of advancement in key policy areas within the region. These findings were instructive, demonstrating more advanced development in frameworks relating to Electronic Transactions, Cybercrime (or "Computer Misuse") and Access to Public Information (Freedom of Information) legislation than evidenced in the other frameworks.

Based upon the results of the comparative law analyses, the regional stakeholders developed baseline policy "building blocks" which – once approved by stakeholders – defined the bases for further policy deliberation and legislative text development. These policy building blocks reaffirmed some common themes and trends found in the international precedents, but also identified particular considerations that would have to be included in the context of a region consisting of sovereign small island developing states. An example of a major situational consideration which impacted deliberations at this and other stages of the process was the question of institutional capacity to facilitate appropriate administration of these new systems.

The policy building blocks were then used to develop customised model legislative texts that meet both international standards and the demand of the HIPCAR beneficiary countries. Each model text was then again evaluated by stakeholders from the perspective of viability and readiness to be translated into regional contexts. As such, the stakeholder group – consisting of a mix of legislative drafters and policy experts from the region – developed texts that best reflect the convergence of international norms with localised considerations. A broad involvement of representatives from almost all 15 HIPCAR beneficiary countries, regulators, operators, regional organizations, civil society and academia ensured that the legislative texts are compatible with the different legal standards in the region. However, it was also recognised that each beneficiary state might have particular preferences with regard to the implementation of certain provisions. Therefore, the model texts also provide optional approaches within the generality of a harmonised framework. This approach aims to facilitate widespread acceptance of the documents and increase the possibility of timely implementation in all beneficiary jurisdictions.

Interaction and Overlapping Coverage of the Model Texts

Due to the nature of the issues under consideration, there are common threads that are reflected by all six frameworks.

In the first instance, consideration should be given to the frameworks that provide for the use of electronic means in communication and the execution of commerce: **Electronic Commerce (Transactions), Electronic Commerce (Evidence), Cybercrime** and **Interception of Communications**. All four frameworks deal with issues related to the treatment of messages transmitted over communications networks, the establishing of appropriate tests to determine the validity of records or documents, and the mainstreaming of systems geared to ensure the equitable treatment of paper-based and electronic material in maltreatment protection, consumer affairs and dispute resolution procedures.

As such, there are several common definitions amongst these frameworks that need to take into account, where necessary, considerations of varying scope of applicability. Common concepts include: "electronic communications network" – which must be aligned to the jurisdiction's existing definition in the prevailing Telecommunications laws; "electronic document" or "electronic record" – which must reflect broad interpretations so as to include for instance audio and video material; and "electronic signatures", "advanced electronic signatures", "certificates", "accredited certificates", "certificate service providers" and "certification authorities" – which all deal with the application of encryption techniques to provide electronic validation of authenticity and the recognition of the technological and economic sector which has developed around the provision of such services.

In this context, **Electronic Commerce (Transactions)** establishes, among other things, the core principles of recognition and attribution necessary for the effectiveness of the other frameworks. Its focus is on defining the fundamental principles which are to be used in determining cases of a civil or commercial nature. This framework is also essential in defining an appropriate market structure and a realistic strategy for sector oversight in the interest of the public and of consumer confidence. Decisions made on the issues related to such an administrative system have a follow-on impact on how electronic signatures are to be procedurally used for evidentiary purposes, and how responsibilities and liabilities defined in the law can be appropriately attributed.

With that presumption of equivalence, this allows the other frameworks to adequately deal with points of departure related to the appropriate treatment of electronic information transfers. The **Cybercrime** framework, for example, defines offences related to the interception of communication, alteration of communication and computer-related fraud. The **Electronic Commerce (Evidence)** framework provides a foundation that introduces electronic evidence as a new category of evidence.

One important common thread linking **e-Transactions** and **Cybercrime** is the determination of the appropriate liability and responsibility of service providers whose services are used in situations of electronically mediated malfeasance. Special attention was paid to the consistency in determining the targeted parties for these relevant sections and ensuring the appropriate application of obligations and the enforcement thereof.

In the case of the frameworks geared to improving regulatory oversight and user confidence, the model texts developed by HIPCAR deal with opposite ends of the same issue: whereas the **Access to Public Information** model deals with encouraging the disclosure of public information with specified exceptions, the **Privacy and Data Protection** model encourages the protection of a subset of that information that would be considered exempted from the former model. Importantly, both these frameworks are geared to encouraging improved document management and record-keeping practices within the public sector and – in the case of the latter framework – some aspects of the private sector as well. It is however notable that – unlike the other four model texts – these frameworks are neither applicable exclusively to the electronic medium nor about creating the enabling framework within which a new media's considerations are transposed over existing procedures. To ensure consistency, frameworks are instead geared to regulating the appropriate management of information resources in both electronic and non-electronic form.

There are a number of sources of structural and logistical overlaps which exist between these two legislative frameworks. Amongst these is in the definition of the key concepts of "public authority" (the persons to whom the frameworks would be applicable), "information", "data" and "document", and the relationship amongst these. Another important form of overlap concerns the appropriate oversight of these frameworks. Both of these frameworks require the establishment of oversight bodies which should be sufficiently independent from outside influence so as to assure the public of the sanctity of their decisions. These independent bodies should also have the capacity to levy fines and/or penalties against parties that undertake activities to frustrate the objectives of either of these frameworks.

In Conclusion

The six HIPCAR model legislative texts provide the project's beneficiary countries with a comprehensive framework to address the most relevant area of regulation with regard to information society issues. They were drafted by reflecting both the most current international standards as well as the demands of small islands developing countries in general and – more specifically – those of HIPCAR's beneficiary countries. The broad involvement of stakeholders from these beneficiary countries in all phases of development of the model legal texts ensures that they can be adopted smoothly and in a timely manner. Although the focus has been on the needs of countries in the Caribbean region, the aforementioned model legislative texts have already been identified as possible guidelines also by certain countries in other regions of the world.

Given the specific and interrelated natures of the HIPCAR model texts, it will be most advantageous for the project's beneficiary countries to develop and introduce legislation based on these models in a coordinated fashion. The Electronic Commerce models (Transactions and Evidence) will function most effectively with the simultaneous development and passage of Cybercrime and Interception of Communications frameworks, as they are so closely related and dependent on each other to address the concerns of robust regulatory development. Similarly, the Access to Public Information and the Privacy and Data Protection frameworks consist of such synergies in administrative frameworks and core skill requirements that simultaneous passage can only strengthen both frameworks in their implementation.

In this way there will be optimal opportunity created to utilise the holistic frameworks that are established in the region.

1.5. This Report

This report deals with Privacy and Data Protection, one of the work areas of the Working Group on the ICT Policy and Legislative Framework on Information Society Issues. It includes Model Policy Guidelines and a Model Legislative Text including Explanatory Notes that countries in the Caribbean may wish to use when developing or updating their own national policies and legislation in this area.

Prior to drafting this document, HIPCAR's team of experts – working closely with the above Working Group members – prepared and reviewed an assessment of existing legislation on information society issues in the fifteen HIPCAR beneficiary countries in the region focusing on six areas: Electronic Transactions, Electronic Evidence in e-Commerce, Privacy and Data Protection, Interception of Communications, Cybercrime, and Access to Public Information (Freedom of Information). This assessment took account of accepted international and regional best practices.

This regional assessment – published separately as a companion document to the current report[3] – involved a comparative analysis of current legislation on Privacy and Data Protection in the HIPCAR beneficiary countries and the identification of potential gaps in this regard, thus providing the basis for the development of the model policy framework and legislative text presented herein. By reflecting national, regional and international best practices and standards while ensuring compatibility with the legal traditions in the Caribbean, the model documents in this report are aimed at meeting and responding to the specific requirements of the region.

[3] See HIPCAR "Privacy and Data Protection: Assessment Report" available at www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/

The model legislative text on Privacy and Data Protection was developed in three phases: (1) the drafting of an assessment report; (2) the development of model policy guidelines; and (3) the drafting of the model legislative text. The assessment report was prepared in two stages by HIPCAR consultants. The first stage was carried out by Ms. Karen Stephen-Dalton, and the second stage by Mr. Kwesi Prescod. The draft documents were then reviewed, discussed and adopted by broad consensus by participants at two consultation workshops for the HIPCAR Working Group on Information Society Issues, held in Saint Lucia on 8-12 March 2010 and in Saint Kitts and Nevis on 19-22 July 2010 (see Annexes). The explanatory notes to the model legislative text in this document were prepared by Mr. Prescod addressing, *inter alia*, the points raised at the second workshop. This document therefore contains data and information as known in July 2010.

Following this process, the documents were finalized and disseminated to all stakeholders for consideration by the governments of the HIPCAR beneficiary countries.

1.6. The Importance of Effective Policies and Legislation on Privacy and Data Protection

Privacy has been identified as a human right, as concretized in various provisions of the Universal Declaration of Human Rights, the International Covenant of Civil and Political Rights, as well as the American and European Convention on Human Rights. This right to privacy which protects the individual's private life against arbitrary, unlawful or abusive interference, by extension provides for the protection of the personal information of the individual, and the protection of the transmission of such information.

Contemporary discussion on privacy and data protection frameworks would be meaningless without discussing the ubiquity of information and communications technology and the capability this provides for the analysis, processing and sharing of information. As businesses seek to utilise new channels to enhance their competitive position in the domestic or global marketplace, user trust that information submitted in the completion of a transaction is protected from use by other parties without their knowledge is critical for the adoption and success of the Internet-based electronic revolution. In this way, the implementation of privacy and data protection frameworks support the objectives of electronic commerce laws by providing a holistic framework to reinforce the needed sense of integrity in the wider regulatory framework, and buttress its ability to protect the customer.

Privacy and Data Protection laws are based on the premise that the individual must have some level of control of how the personal information collected from them by the government or businesses are utilised, processed or disclosed. This control is primarily asserted at the point at which information is collected, at which time the collecting party must make a full disclosure of the intent for which the information is to be collected, and be commit to be so constrained in the use of the personal information after it is collected. The other major facilitation of the individual's control is the obligation of the collecting party to provide the individual with the opportunity to review any information which is stored by the party about the individual. Despite this, there should be exemptions to the general rules associated with the restriction of the use of personal information, with the application of specific, different guidelines in the fields of medical services and national security where gaining the assent of the individual is not practical.

As such, policies and legislative frameworks treating with privacy and data protection are geared to treating with the management of private and personal information only. In this way, such frameworks work in concert with rules treating with the government giving access to the public, non-sensitive information it possesses, as such frameworks generally do not treat with the management of personal information other than the general exemptions from the provisions of those laws.

While there should be particular consideration of the oversight of government, Privacy and Data Protection frameworks should not be limited to the Public Sector, but should encompass all parties that, as a matter of business, collect, store and analyse personal information of customers. Privacy and Data

Protection laws are critical for the meaningful establishment of e-government systems geared to enhancing efficiency of the provision of government goods and services, as well as enhancing the economic competitiveness of the commercial sector.

Government bodies and other agencies in the provision of public services have traditionally, as a course of their mandate, utilised personal information of customers in the public. However, with the move towards greater transparency and equity in the management of government affairs there are a number of concerns relating to how this information is to be used. These concerns may vary from limiting the influence of unfair prejudice due to race, religion, ethnicity, gender or sexual orientation in the allocation of public resources, goods or services that are not directly related to these characteristics, to concerns relating to the systems in place to protect stored information from unauthorised access by other parties. As such, just as there has been the obligation to establish frameworks to minimise the consideration of private characteristics in the evaluation of access to public resources, unless these characteristic are, in law, the substantive discretionary factor in the evaluation process, there must also be protection against unauthorised disclosure or access to personal information by ensuring some appropriate minimum standards of information security are deployed.

From the perspective of the private sector, customers require ever more assurance that personal information garnered in the conduct of a particular business transaction is not used, or misused by third parties. Such assurance must limit the sale or otherwise disclosure of personal information to third parties without the knowledge, and tacit approval of the individual.

Privacy and Data Protection laws must also recognise the emerging nature of electronic commerce, and the impetus for cross border information transfers. Businesses that leverage information and communications technologies tend to seek opportunities to rationalise investment so as to reduce cost and increase efficiencies. In many instances such strategies include the aggregation of information collected in the course of business to single locations. In the case of multi-national firms, this impetus usually means the aggregation of business information from multiple countries at a single location that may not be situated within any of the jurisdictions from which the information is garnered. In this instance, if the rules regarding the protection of personal information are not as stringent as those of the country where the firm collects the information, this imbalance may result in the compromising of the privacy of persons in the substantive jurisdictions of operation. This is so critical a point, that reciprocal protection of personal information is a major component of contemporary trade agreements between nations, and/ or regulatory restrictions imposed on multi-national firms. Implementation of privacy and data protection rules then affords countries the opportunity to enter, partake and benefit in new areas of economic endeavour in international trade, relating to distance and remote service provision.

Finally, there is recent discussion of the economic opportunity associated with the control, use and analysis of information collected by Internet content aggregators or marketing enterprises. This has led to the discussion of the “personal information value chain”, and the recognition of the economic potential associated with the various actors along this chain. In the heart of this framework for the new information economy is the recognition of the rights of the individual to exert control over how particular personal information is to be used. Therefore, as the Internet economic revolution gathers momentum, the implementation and enforcement, and thus the credibility, of the Privacy and Data Protection rules of a jurisdiction shall become a key competitive advantage for that jurisdiction as a focus of investment in this burgeoning area of business activity - which largely involves the management of personal information.

Therefore, the implementation of effective policies, legislation and systems to ensure Privacy and Data Protection provides substantial multi-faceted benefits to a country that redounds to the improvement of governance and democracy, as well as prepares the country, and the businesses based there, to leverage new opportunities in the information age. The implementation of such policies, legislation and systems must reflect administrative frameworks that limit the potential for undue interference of either the Executive arm of the State or commercial enterprise to reinforce the importance of privacy and data protection to the rules and principles of good governance.

Section I: Model Policy Guidelines – Privacy and Data Protection

Following, are the Model Policy Guidelines that a country may wish to consider in relation to Privacy and Data Protection.

1. CARICOM/CARIFORUM COUNTRIES SHALL AIM TO INTRODUCE CLEAR LEGAL AND INSTITUTIONAL FRAMEWORKS TO ENSURE THE PROTECTION OF PERSONAL AND PRIVATE INFORMATION

- There is a clear legal mandate in law to support the establishment of a regime to ensure protection of personal and/ or private information.
- The regime of data protection should not be technology specific, and should therefore have equal relevance in the paper-based or ICT-enabled environments.
- The law/legal mandate should clearly state that the law binds the State.
- The law/legal mandate should ensure that the obligation of privacy protection is applied by both the Public and Private sectors.
- The law/legal mandate clearly identifies a designated agency for the implementation of the Privacy and Data Protection framework.
- The law/legal mandate clearly provides for the independence of the designated agency.
- The law/legal mandate clearly provides that personal information should be collected and processed with the consent of the subject of the personal information.
- The law/legal mandate clearly specifies the circumstances under which personal information can be collected and processed without the consent or notification of the subject of the personal information.
- The law/legal mandate should identify a category of personal information as “sensitive information”, requiring more stringent oversight and control.

2. CARICOM/CARIFORUM COUNTRIES SHALL ENSURE THAT KEY PRINCIPLES OF DATA PROTECTION ARE CLEARLY DEFINED IN THE RELEVANT ACTS

- Key principles of the Data Protection framework are clearly defined in the Acts.
- Among the Key Principles of Data Protection should be such provisions to ensure that at the time of collection the data subject is made aware of the purpose/use of such data and clearly consents to such purpose/use of said data.
- Among the Key Principles of Data Protection should be such provisions to place the responsibility on the person and/or entity collecting and/ or processing the personal information for the security, accuracy and appropriate usage of that information.
- Among the Key Principles of Data Protection should be such provisions to engender confidence in the public by allowing the data subject to review and ensure accuracy of information kept about them by any person.
- Among the Key Principles of Data Protection should be such provisions to limit the trans-border transfer of personal information to jurisdictions that do not share comparable safeguards of privacy and data protection.

3. CARICOM/CARIFORUM COUNTRIES SHALL AIM TO ESTABLISH APPROPRIATE GOVERNANCE FRAMEWORKS PROVIDING INSTITUTIONS WITH APPROPRIATE POWERS TO FACILITATE OVERSIGHT

- The law/legal mandate shall clearly stipulate that there be provisions for the clear identification of the collectors, users and processors of personal information such provision may include notification to or registration with the designated person.
- The agency designated to ensure compliance with the law/legal mandate shall be a distinct legal person with the power to own or dispose of assets, the ability to enter into contracts, and who shall be independent in the performance of its functions.
- The Head of the designated agency shall be appointed in a manner to ensure independence and impartiality of functions.
- The Head of the designated agency shall be afforded such terms and conditions of employment, including provisions of entrenchment and conditions of reappointment, included in the law/legal mandate that are sufficient to limit the opportunity for inducement or coercion.
- The Head of the designated agency shall be afforded in the law/legal mandate the necessary powers of investigation to facilitate the execution of the functions of the Data Protection framework.
- The Head of the designated agency shall be afforded in the law/legal mandate the power to delegate certain authority to recognized agents to facilitate the execution of his function.
- The designated agency may undertake audits or investigations into the operations of persons to whom the framework is applicable, either on its own accord or in response to complaints from the public. The person who shall bear the burden of cost of such audits or investigations shall be determined in Regulations.
- Persons to whom the law applies shall cooperate with the designated agency in the exercise of its functions, under the penalty of civil and/or criminal penalties.
- The designated agency may make requests, to which relevant persons must comply, for the submission of certain documents to facilitate its investigations. The agency may gain a warrant from the Courts to achieve such if it is warranted.
- In the law/legal mandate, the designated agency may be provided protection from liability for any acts done in good faith in the exercise of its function.
- The designated agency shall report annually to the Parliament/Legislative Council on its operations for the year prior.
- The law/legal mandate shall specify a timeframe in which the designated agency will come into force upon passage of the Act.

4. CARICOM/CARIFORUM COUNTRIES SHALL OUTLINE PARTICULAR REQUIREMENTS AND OBLIGATIONS WITH REGARD TO THE COLLECTION OF PERSONAL INFORMATION

- The law/legal mandate shall reinforce that public authorities only collect personal information that is expressly authorized by a written law.
- The law/legal mandate shall provide for the explicit notification of the data subject of the purpose for which personal information is collected, and that the information collected is relevant to the purpose.
- The law/legal mandate shall provide for the data subject to explicitly consent to the collection of information.
- The law/legal mandate provides for the collection of personal information from the data subject only, subject to specified exemptions associated with concerns of national security or health management.
- The law/legal mandate shall provide for exemptions that are clear, precise and limited so that there remains adequate protections for the data subject against unwarranted data collection.
  - In associated law or regulations, there shall be outlined specific considerations to ensure that there are adequate checks and balances to the access and use of personal information with regard to the exemptions identified in the general Privacy and Data Protection Acts.
- The law/legal mandate provides that the data subject should be informed at the time of data collection, of the person who will control the data, the expected period of retention of that data and the manner of disposal of the data upon expiration of the retention period except in circumstances of health management and national security.
- The law/legal mandate limits the collection of sensitive personal information except for specified instances and purposes. Such exemptions may include:
  - The development of statistics;
  - Health management;
  - Law enforcement requirements;
  - Requirements of a rule of law;
  - Requirements of a Court order.
- The law/legal mandate prescribes civil and criminal penalties for the breach of the defined provisions relating to the collection of personal information. Such penalties may be levied against the collecting party, or any officer or director that can be proven to have willfully breached the law/legal mandate.

Section I

5. CARICOM/CARIFORUM COUNTRIES SHALL OUTLINE PARTICULAR REQUIREMENTS AND OBLIGATIONS WITH REGARD TO THE PROCESSING OF PERSONAL INFORMATION

- The law/legal mandate limits the collecting party from the use or processing of information to the purposes specified and consented to by the data subject at the point of collection.
- The law/legal mandate limits the retention of collected information to a period necessary for the purpose specified.
- The law/legal mandate obliges the party using the information ("the processing party") to ensure it accurately records and processes that information.
- The law/legal mandate obliges the processing party to safeguard the information stored by undertaking appropriate systems to provide adequate security.
- The law/legal mandate requires the processing party to seek the review and approval of the designated agency before undertaking particular types of processing.
- The law/legal mandate provides for the data subject having access, on request, to the personal information retained about that data subject by the processing party.
- The law/legal mandate provides the head of the processing party with the discretion to reject an application for access to stored information on a data subject if:
    - the release of the information will compromise the anonymity of another person;
    - the request is vexatious in nature and overly disruptive to operations.
- The law/legal mandate provides for the appeal of decisions of the head of the processing party to the designated agency.
- The law/legal mandate prohibits the processing of sensitive personal information, except for specified instances and purposes. Such exemptions may include:
    - Statistics;
    - Health management;
    - Law enforcement requirements;
    - Requirements of a rule of law;
    - Requirements of a Court order.
- The law/legal mandate prescribes civil and criminal penalties for the breach of the defined provisions relating to the collection of personal information. Such penalties may be levied against the collecting party, or any officer or director that can be proven to have willfully breached the law/legal mandate.

6. CARICOM/CARIFORUM COUNTRIES SHALL OUTLINE PARTICULAR REQUIREMENTS AND OBLIGATIONS WITH REGARD TO THE DISCLOSURE OF PERSONAL INFORMATION

- The law/legal mandate obliges the party who collects, processes or uses personal information not to disclose that personal information without first obtaining consent from the data subject.
- The law/legal mandate provides for the exemption of the obligation for consent of the data subject where required by a rule of law, if related to concerns of national security, provision of justice and health management.
- The law/legal mandate limits the trans-border transfer of personal information to jurisdictions without comparable personal and data protection laws and systems. In such an instance, the law provides for a transfer of information only as much as will not result in a compromise of the protection of the data subject information.
- The law/legal mandate provides, notwithstanding any standards restriction, that the transfer of personal information may be facilitated with the express consent of the data subject to transfer the information to that jurisdiction, pursuant to the data subject being notified of the attendant risks.
- The law/legal mandate provides for the disclosure of personal information in response to a request from the data subject. Where such disclosure may result in the disclosure of other restricted information, the law/ legal mandate shall prescribe appropriate guidance to the Head of the processing party.
- The law/legal mandate prescribes civil and criminal penalties for the breach of the defined provisions relating to the disclosure of personal information. Such penalties may be levied against the processing party, or any officer or director that can be proven to have breached the obligations of the law/legal mandate.

Section II: Model Legislative Text – Privacy and Data Protection

Following, is the Model Legislative Text that a country may wish to consider when developing national legislation relating to Privacy and Data Protection. This model text is based on the Model Policy Guidelines outlined previously.

Arrangement of Sections

PART I – PRELIMINARY

Short Title and Commencement

1. This Law may be cited as the "Privacy and Data Protection Act", and shall come into force and effect [on xxx following publication in the *Gazette*].

Objective

2. The objective of this Act is to provide an enabling legal framework to support the development of culture and practice of privacy protection through:

   a. Defining general principles by which personal information of an individual is to be treated;

   b. Defining management guidelines (including systems and technology) by which persons which manage personal information will adhere; and

   c. Establishing an administrative framework to ensure transparent oversight, and impartial dispute resolution that will strengthen the protection of personal information by both the public and private sector.

Definitions

3. (1) In this Act, the following words and phrases shall have the meanings assigned thereto hereunder:

   a. "data" or "information" means any record, document, correspondence, memorandum, book, plan, map, drawing, pictorial or graphic work, photograph, film, microfilm, sound recording, videotape, machine-readable record and any other documentary material, regardless of physical form or characteristics, and any copy of those things.

   b. "data commissioner" means the data commissioner appointed under Part VII, Section 49 of this Act.

   c. Data Controller" means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, collected, processed or disclosed.

   d. "data subject" means an individual who is the subject of personal data.

   e. "Minister" means the Minister who has been assigned responsibility for [information/public administration].

   f. "health care institution" refers to institutions registered as facilities for the provision of health care in accordance with [relevant Public Health Care Law] and includes hospitals, health centres, clinics [and doctor's offices].

   g. "health care professional" means a professional registered to practice medicine in accordance with [relevant Public Health Care Law].

   h. "personal information" means information about an identifiable individual that is recorded in any form including—

      i. information relating to the nationality, address, age or marital status of the individual;

ii. information on the racial or ethnic origins of the individual;

iii. information on the political opinions or affiliations of the individual;

iv. information on religious beliefs or other beliefs of a similar nature of the individual;

v. information relating to physical or mental health or condition of the individual;

vi. information related to bio-metrics of the individual

vii. information related to the sexual orientation or sexual life of the individual; or

viii. information related to the criminal or financial record of the individual;

ix. information relating to the education, or employment history of the individual;

x. any identifying number, symbol or other particular designed to identify the individual;

xi. the views and opinions of any other person about the individual.

i. public authorities” include -

i. a House of Parliament or a committee of any House of Parliament;

ii. the Cabinet as constituted under the Constitution;

iii. a Ministry or a department or division of a Ministry,

iv. a local authority;

v. a public statutory corporation or body;

vi. a body corporate or an incorporated body established for a public purpose, which is owned or controlled by the state;

vii. any other body designated by the Minister by regulation made under this Act, to be a public authority for the purposes of this *Act*.

j. “processing”, “processed”, in relation to data, means obtaining, recording or holding the data or carrying out any operation or set of operations on data, including –

i. organization, adaptation or alteration of the data;

ii. retrieval, consultation or use of the data; or

iii. alignment, combination, blocking, erasure or destruction of the data.

k. “relevant filing system” means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

(2) Where the member state believes it warranted to define a particular set of sensitive personal information it may do so as below:

a. "sensitive personal information" means information on a person's—
   i. racial or ethnic origins;
   ii. political opinions;
   iii. religious beliefs or other beliefs of a similar nature;
   iv. physical or mental health or condition;
   v. sexual orientation or sexual life; or
   vi. criminal or financial record;

Binds the State

4. This Act shall bind the State.

Applicability of the Act

5. This Act applies to a the Data Controller in respect of any data if-

a. the Data Controller is established (ordinarily resident, incorporated or branch office) in [Name of Member State] and the data is processed in the context of the business of that establishment; or

b. the Data Controller is not established in [Name of Member State] but uses equipment in [Name of Member State] for processing data otherwise than for the purpose of transit through [Name of Member State].

Non-Applicability of the Act

6. This Act shall not –

a. limit information available by law to a party in any proceeding;

b. limit the power of a court or tribunal to compel a witness to testify or to compel the production of a document or other evidence; or

c. apply to notes prepared by or for an individual presiding in a court of [country] or in a tribunal if those notes are prepared for that individual's personal use in connection with the proceedings.

General Privacy Principles

7. Pursuant to this Act, all persons that treat with personal data in the conduct of business shall be responsible for their adherence to the following general principles:

a. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless particular conditions have been met.

b. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

c. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

d. Personal data shall be accurate and, where necessary, kept up to date.

e. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

f. Personal data shall be processed in accordance with the rights of data subjects under this Act.

g. Appropriate technical and institutional measures shall be taken against unlawful processing of personal data and against accidental loss or destruction of, or damage to, such data.

h. Personal data shall not be transferred to a country or territory outside the [*name of jurisdiction*] unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

PART II – OBLIGATIONS OF THE DATA CONTROLLERS

Limitation on the Collection and Processing of Personal Information

8. (1) No person shall cause the collection and or processing of personal data unless an entry in respect of that person as the Data Controller is included in the register maintained by Commissioner.

(2) Personal information may not be collected by or for the Data Controller unless—

a. the collection of that information is considered fair, and necessary as part of an agreement between the Data Controller and the data subject;

b. the collection is expressly authorized by or under any written law.

Personal Information to be Collected Directly

9. (1) Where the Data Controller requires personal information from an individual it shall cause the personal information to be collected directly from that individual with their explicit consent.

(2) The data subject, except where otherwise provided in any other law, shall be entitled to object at any time to the Data Controller on compelling legitimate grounds to the processing of such data.

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

a. another method of collection is authorized by the individual, by the Data Commissioner or by any other written law; and

b. the information is collected for the purpose of -

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

   ii. proceedings before a court or a judicial or quasi-judicial tribunal;

   iii. collecting a debt or fine or making a payment; or

   iv. law enforcement.

Data Subject to be Informed of Purpose

10. At the time of collection of personal data or before, the Data Controller shall ensure that the data subject is informed of -

a. the purpose for collecting it;

b. the intended recipients;

c. whether providing answers to questions are voluntary or compulsory and the possible consequences of failure to reply;

d. where applicable, the legal authority for collecting it; and

e. the title, business address, telephone number and other contacts of an official of the Data Controller who can answer the data subject's questions about the collection.

Retention of Personal Information

11. Personal information that has been used by the Data Controller for an administrative purpose shall be retained by the Data Controller only for such period of time after it has been used as may be prescribed by Regulations, to ensure that the data subject has a reasonable opportunity to obtain access to that information.

Disposal of Personal Information

12. The Data Controller shall dispose of all personal information in its control or custody in accordance with Regulations made by the Minister under this Act.

Accuracy of Personal Information

13. The Data Controller shall make every reasonable effort to ensure that the personal information in its custody of a given data subject is accurate and complete.

Protection of Personal Information

14. (1) The Data Controller shall protect personal information in its custody or under its control by making reasonable technical and institutional security arrangements against such risks as unauthorized access, collection, use, alteration, disclosure or accidental disposal.

(2) Where any other person processes personal information on behalf of the Data Controller, the data the Data Controller shall ensure that the person:

a. can implement the security measures that must be taken;

b. actually takes the measures so identified by the data the Data Controller.

Processing of Personal Information Consistent With Purpose

15. (1) Personal information under the custody or control of the Data Controller shall not, without the consent of the individual to whom it relates, be processed except for the purpose for which the information was obtained or compiled by the data the Data Controller, or for a use consistent with that purpose.

(2) The processing of personal information is consistent with the purposes for which it was obtained if the processing has a reasonable and direct connection to the purpose, and that purpose is in accordance with the criteria outlined in subsection (3).

(3) Personal information may be processed only if:

a. the data subject has unambiguously given his consent; or

b. by a health care professional performing necessary duties at a health care institution;

c. where it has been made public by the data subject;

d. for research and statistical purposes in accordance with section 17;

e. in the interest of law enforcement and national security; or

f. for the purposes of determining access to social services.

g. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

h. processing is necessary for compliance with a legal obligation to which the Data Controller is subject; or

i. processing is necessary in order to protect the vital interests of the data subject; or

j. processing is necessary for the performance of an activity that is carried out in the public interest or in the exercise of official authority vested in the Data Controller or in a third party to whom the data is disclosed; or

k. processing is necessary for a purpose that concerns a legitimate interest of the Data Controller or of such a third party to whom personal data is provided, except where such interest is overridden by the interest to protect the right to privacy of the data subject.

(4) Where the jurisdiction believes it necessary to distinguish "sensitive personal information" it may further limit the collection and processing of such information, with exemptions associated with (b) through (f) above.

Disclosure of Personal Information

16. Except as provided under any other written law, personal information under the control of the Data Controller may only be disclosed -

a. for the purposes for which the information was collected by the data the Data Controller or for a use consistent with that purpose;

b. for any purpose in accordance with any written law or any order made pursuant to such written law that authorizes such disclosure;

c. for the purpose of complying with a subpoena or warrant issued or order made by a court, person or body with jurisdiction to compel the production of information or for the purpose of complying with rules of court relating to the production of information;

d. to the Attorney General of [name of jurisdiction] for use in legal proceedings involving the State

e. to an investigative body specified by the Minister by Order, on the written request of the investigative body, for the purpose of investigating compliance with any written law or carrying out a lawful investigation, if the request specifies the purpose and describes the information to be provided;

f. by one law enforcement agency in [name of jurisdiction] to another law enforcement agency within [name of jurisdiction] for the purpose of enforcement of a written law;

g. to a law enforcement agency in a foreign country under a written agreement, treaty or under the authority of the Government of [name of jurisdiction];

h. if the head of the Data Controller agrees that a compelling circumstance exists that affects the health or safety of any person and if, subject to Section 23 (d), notice of the disclosure is mailed to the last known address of the data subject,

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 a data subject to the Government of [name of jurisdiction] or to the Data Controller;

k. for statistical purposes where the disclosure meets the requirements of section 17; or

l. for archival purposes where the disclosure meets the requirements of section 18.

Disclosure for Research or Statistics

17. The Data Controller may cause personal information in its custody or control to be disclosed for a research purpose, including statistical research only if –

a. the research purpose cannot reasonably be accomplished unless that information is provided in individually identifiable form;

b. the information is disclosed on condition that it not be used for the purpose of contacting a person to participate in research;

c. any recorded linkage is not harmful to the data subject and the benefits to be derived from the record linkage are clearly in the public interest;

d. the head of the Data Controller concerned has approved conditions relating to the following:

   i. security and confidentiality;

   ii. the removal or destruction of the individual identifiers at the earliest reasonable time;

   iii. the prohibition of any subsequent use or disclosure of that information in individually identifiable form without the express authorization of that the Data Controller; and

e. the person to whom that information is disclosed has signed an agreement to comply with the approved conditions, this Act and any of the Data Controller's policies and procedures relating to the confidentiality of personal information.

Disclosure for Archival Purposes

18. The National Archives of the Government of [name of jurisdiction] or the archives of the Data Controller may disclose personal information or cause personal information in its custody or control to be disclosed for archival or historical purposes if -

a. the disclosure would not be an unreasonable invasion of professional or personal privacy;

b. the disclosure is for historical research and is in accordance with section 18;

c. the information concerns someone who has been deceased for [...] or more years; or

d. the information is in a record that has been in existence for one [...] or more years.

Restriction of Transfer to Third Party Jurisdictions

19. (1) Without prejudice to the provisions of the following, the transfer to a third party jurisdiction of personal data that is to undergo processing may only take place subject to the provisions of this Act and provided that the third party jurisdiction to which the data is to be transferred ensures comparable levels of protection.

(2) The adequacy of the level of protection of a third party jurisdiction shall be assessed in the light of all the circumstances surrounding a data transfer operation or a set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third party country and the professional rules and security measures which are complied with in that country.

(3) The Data Commissioner shall make a determination as to whether a third party country ensures an adequate level of protection. Upon the making of such a determination, the Data Commissioner shall make known:

a. the relevant public authority with responsibility for Data Protection in the other jurisdiction;

b. his determination of the comparable levels of protection provided; and

c. where protections are determined to be incompatible, the aspects of personal information [and sensitive personal information] which would not be appropriately protected.

(4) Where, despite non comparable levels of protection, the Data Commissioner determines that some limited form of transfer may be facilitated which would limit the breach of the data subject's rights in accordance with this Act, the Data Commissioner may authorise such a transfer where:

a. the data subject consents to the transfer of the information to the third party jurisdiction; and

b. there is appropriate severance or redaction of those aspects of the information which the Data Commissioner deems appropriate.

(5) [Where there is an existing arrangement for processing of the data or information in a third party jurisdiction a reasonable period of transition may be allowed for by the Commissioner to enable the data controller to move the processing to another jurisdiction if so required.]

(6) Subject to subsections (4) and (5), the transfer of personal data to a third party jurisdiction that does not ensure adequate protection is prohibited.

Codes of Practice

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

a. providing guidance on the development of codes of practice;

b. providing guidance on compliant resolution mechanisms;

c. fostering education on the General Privacy Principles;

d. working with government and private sector bodies to promote awareness of codes of conduct among consumers; and

e. taking any action that appears to the Data Commissioner to be appropriate.

Mandatory Codes of Practice

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

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

PART III – RIGHTS OF THE DATA SUBJECT

Right of Access to Own Personal Information

22. (1) Every individual who is a citizen of or resident in [name of jurisdiction] has a right to and shall on request, and upon payment of the prescribed fee be given access to -

a. personal information about that individual contained in a personal information filing system in the custody and control of the Data Controller;

b. any other personal information about the individual under the custody or control of a data the Data Controller with respect to which the individual is able to provide sufficiently specific information as to render it reasonably retrievable by the Data Controller.

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

Data Controller may Refuse Access

23. (1) The Data Controller may refuse to disclose personal information to the individual to whom the information relates where -

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

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

c. it is information that is subject to legal privilege or obtained in the course of an investigation or legal proceeding,

d. it is health or medical information where the head of the Data Controller has a reasonable belief that providing access to the information could harm the health or safety of any person;

e. it is evaluative or opinion material compiled solely for the purpose of determining suitability or eligibility for employment, the award of government contracts and other benefits where the disclosure would reveal the identity of a source who furnished information in circumstances where it may reasonably be assumed that the identity of the source would be held in confidence.

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

Severance of Exempt Information

24. (1) The Data Controller shall make every effort to sever information that is exempt from disclosure pursuant to section 24 from information that may be made available to the individual requesting access to his personal information and make the non-exempt information available.

(2) The head of the Data Controller may refuse to disclose the existence of information where acknowledgment of such existence would reveal critical aspects about the exempt nature of the information.

Delegation of Rights of Data Subject

25. Any right or power conferred on an individual by this Act 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;

c. the individual's guardian; or

d. where the individual is less than eighteen years of age, by a person who has lawful custody of the individual.

Time Limits for Response to Request

26. (1) Where a request is made for access to personal information pursuant to section 23, the head of the Data Controller shall, within [...] days after the request is received -

grant access in whole or in part, giving the information to the individual who made the request; or

refuse to grant access in whole or in part, giving the individual who made the request a written response stating -

i. that the information does not exist; or

ii. the specific provision of the Act on which a refusal could reasonably be expected to be based if the information existed; and

iii. information regarding the right of appeal to the Data Commissioner.

(2) Where access is granted in whole or in part, the head of the Data Controller shall ensure that the information is available in a comprehensive form, including where reasonable, comprehensible to an individual with a sensory disability.

Correction of Errors in Stored Personal Information

27. (1) Where an individual believes there is an error or omission in his personal information, the individual may request the head of the data the Data Controller that has the information in its custody or under its control, to correct the information.

(2) If no correction is made in response to a request under subsection (1), the head of the data the Data Controller shall annotate the information with the correction that was requested but not made and notify the individual who made the request that no correction was made.

Section II

(3) On correcting or annotating personal information under this section, the head of the Data Controller shall notify any other the Data Controller or any third party to whom that information has been disclosed during the one-year period before the correction was requested, of such correction or annotation.

(4) Upon being notified under subsection (3) of a correction or annotation of personal information, the Data Controller shall make the correction or annotation on any record of that information in its custody or control.

PART IV – PARTICULAR OBLIGATIONS OF PUBLIC AUTHORITIES

Privacy Impact Assessments

28. (1) Every Ministry shall prepare a privacy impact assessment, in the form prescribed by the Data Commissioner, for any proposed enactment, system, project, programme or activity.

(2) Upon preparation of a privacy impact assessment, every Ministry shall submit such privacy impact assessment to the Data Commissioner for approval.

(3) Where a privacy impact assessment has been submitted in accordance with subsection (2) the Data Commissioner shall evaluate such privacy impact assessment in accordance with the General Privacy Principles and where necessary, make recommendations to the Ministry for amendments to assure compliance.

(4) Where the Data Commissioner makes a recommendation under subsection (3), the Ministry shall make the necessary amendments to its proposed enactment, system, project, programme or activity.

(5) Every Ministry shall take all reasonable steps in accordance with its privacy impact assessment to avoid unnecessary intrusions into personal privacy when designing, implementing or enforcing enactments, systems, projects, programmes or activities.

Personal Information Filing Systems

29. The head of a public authority who is a registered the Data Controller shall cause to be included in personal information filing systems, all personal information under the control or in the custody of the Data Controller that -

a. has been processed, is being processed or is available for use for an administrative purpose; or

b. is organized or intended to be retrieved by means of the name of an individual or by an identifying number, symbol or other particular assigned to an individual.

Exemption of the National Archives

30. Notwithstanding section 31, personal information under the custody or control of the Archives of the Government of [name of jurisdictions] that has been transferred to it by a public authority for historical or archival purposes shall not be included in personal information banks.

Personal Data Representative

31. (1) The Data Controller shall notify the Data Commissioner on the appointment or removal of a personal data representative.

(2) The personal data representative shall have the function of independently ensuring that the Data Controller processes personal data in a lawful and correct manner and in accordance with goodpractice and in the event of the personal data representative identifying any inadequacies, he shall bring these to the attention of the Data Controller.

(3) If the personal data representative has reason to suspect that the Data Controller has contravened the provisions applicable for processing personal data and if rectification is not implemented as soon as practicable after such contravention has been pointed out, the personal data representative shall notify this situation to the Data Commissioner.

Information Sharing to be Authorised

32. Where a public authority intends to share information with other public authorities, it shall do so only pursuant to an agreement in a manner prescribed by the Data Commissioner, and thereby approved.

Commissioner to Publish Report on Personal Information Banks

33. The Data Commissioner shall publish periodically, but not less than annually, an index of the personal information that is held by the public authorities that includes a summary of the following:

a. the personal information filing systems 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 Data 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; and

g. privacy impact assessments prepared by any Ministry.

PART V – SPECIAL EXEMPTIONS

Domestic Purpose

34. An individual is exempt from the provisions of Parts 3, 4 and 5 where the data is processed by the individual only for the purposes of that individual's personal, family or household affairs or for recreational purposes.

National Security, Crime and Taxation

35. (1) The Minister may by Order published in the Gazette exempt a data the Data Controller from complying with any provision of this Act in the interest of national security.

(2) A data the Data Controller which is a public authority shall be exempt from the provisions of [Parts II and III] if the processing of data is required for –

a. the prevention or detection of crime;

b. the apprehension or prosecution of offenders; or

c. the assessment or collection of any tax, duty or any imposition of a similar nature.

Exemptions on Applicability to Regulatory Activities

36. (1) Personal data processed for the purposes of discharging functions pursuant to regulatory activities required of any written law are exempt from Part II and III of this Law in any case to the extent to which the application of those provisions to the data would be likely to prejudice the proper discharge of those functions.

(2) Subsection (1) applies to any relevant function which is designed —

a. for protecting members of the public against —

   i. financial loss due to dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment or other financial services or in the management of bodies corporate,

   ii. financial loss due to the conduct of discharged or undischarged bankrupts, or

   iii. dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons authorised to carry on any profession or other activity,

b. for protecting charities against misconduct or mismanagement (whether by trustees or other persons) in their administration,

c. for protecting the property of charities from loss or misapplication,

d. for the recovery of the property of charities,

e. for securing the health, safety and welfare of persons at work, or

f. for protecting persons other than persons at work against risk to health or safety arising out of or in connection with the actions of persons at work.

Exemptions on Applicability to Journalism, Literature and Art

37. (1) Where personal information is to be processed in the particular circumstance where -

a. the processing is undertaken with a view to the publication by any person of any journalistic, literary or artistic material;

b. the Data Controller reasonably believes that, having regard in particular to the special importance of the public interest in freedom of expression, publication would be in the public interest; and

c. the Data Controller reasonably believes that, in full consideration of the circumstance, compliance with the relevant provisions of Part II is incompatible with the journalistic, literary or artistic purposes to be undertaken,

that personal information will be exempt from Parts II and III of this Law.

(2) To provide for subsection (1) the Data Commissioner may establish codes of conduct in accordance with Sections 21 and 22, which may modify where appropriate the provisions of Parts II and III so as to achieve an appropriate balance of the objects of this Act and the prevailing right of freedom of expression.

PART VI – REVIEW AND APPEALS

Right of an Applicant to Appeal the Decision of the Data Controller

38. An individual who has filed a request for his personal information pursuant to section 23 or who has requested correction of personal information pursuant to section 28 may appeal any decision of the head of the Data Controller to the Data Commissioner.

Time Limit for Appeal to be Lodged

39. An appeal to the Data Commissioner under section 39 shall be made within [...] weeks of the date when the notice was given of the decision appealed from, by filing with the Data Commissioner a written notice of appeal.

Commissioner may Dismiss an Appeal

40. The Data 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.

Commissioner to notify data the Data Controller of Appeal

41. Upon receiving the notice of appeal, the Data Commissioner shall inform the head of the data the Data Controller concerned and any other affected person of the notice of appeal.

The Data Commissioner may Authorise a Mediator

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

Commissioner may Conduct an Enquiry

43. (1) The Data Commissioner may conduct an enquiry to review the decision of the head of the Data Controller if the Data Commissioner has -

a. not authorized a mediator to conduct an investigation under section 43; or

b. authorized a mediator to conduct an investigation under section 43, but no settlement has been reached.

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

a. affirm the decision of the head of the Data Controller; or

b. order the head of the Data Controller to release the personal information or make the corrections requested.

Meetings Conducted in Private

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

Representa-tion at Enquiry

45. An individual who appeals a refusal of access to personal information, the head of the Data Controller concerned and any affected party may be represented by counsel or an agent.

Burden of Proof with the Data the Data Controller

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

Appeal to the Courts

47. Either party may appeal the decision of the Data Commissioner to the Courts in accordance with Section 80 of this Act.

PART VII – OFFICE OF THE DATA COMMISSIONER

Establishment of the Office of the Data Commissioner

48. (1) Subject to subsection (2), there shall be a Data Commissioner who shall be appointed by the [Head of State] after consultation with the Prime Minister and the Leader of the Opposition.

(2) A person is not qualified to hold office as Commissioner if he -

a. is a Minister, Parliamentary Secretary, or a Member of the House of Assembly; or

b. is a judge or magistrate; or

c. is a public officer; or

d. is a member of a local authority; or

e. has a financial or other interest in any enterprise or activity which is likely to affect the discharge of his functions as a Commissioner; or

f. is an undischarged bankrupt; or

g. has at any time been convicted of any offence involving dishonesty.

(3) The Data Commissioner shall be employ staff as may be necessary who shall be under the administrative control of the Data Commissioner.

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

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

h. the Data Commissioner resigns or if his office is otherwise vacant;

i. the Data Commissioner is for any reason unable to perform the functions of his office;

j. the Data Commissioner considers it necessary, on a temporary basis, not to carry out any of his functions because of such circumstances, that were he a judge of the High Court, he would abstain

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

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

Legal Personality and Representation of the Data Commissioner

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

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

Tenure of Office

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

(2) Subject to the provisions of subsection (3), the Data Commissioner vacates his office-

a. at the expiration of the term for which he was appointed;

b. if he becomes disqualified by virtue of subsection 49(2) or

c. if he is appointed to any other office of emolument or engages in any other occupation for reward;

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

Remuneration of Data Commissioner and Staff

51. The Data Commissioner and his staff shall be paid such remuneration and allowances for expenses, out of moneys provided from the Consolidated Fund.

Protection of the Data Commissioner

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

Delegation of Powers by Commissioner

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

Independence of Functions

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

Functions of the Data Commissioner

55. The Data Commissioner shall-

a. ensure compliance with this Act and the Regulations;

b. create and maintain a register of the Data Controllers;

c. exercise control on all data processing activities and either of his own motion or at the request of a data subject, verify whether the processing of data is carried on in accordance with the provisions of this Act or the Regulations;

d. instruct the Data Controller to take such measures as may be necessary to ensure that the processing of data is in accordance with this Act or the Regulations; and

e. investigate reports and claims from data subjects or associations representing data subjects on violations of this Act or the Regulations and take remedial action as the Data Commissioner deems necessary or as may be prescribed under this Act, and to inform the data subjects or associations of the outcome;

f. issue such directions or public statements as may be required of the Data Commissioner for the purposes of this Act;

g. take such measures as may be necessary so as to bring the provisions of this Act to the knowledge of the general public;

h. promote by education and publicity, an understanding and acceptance of the data protection principles and of the objects of those principles;

i. advise the Government on any legislative measures that are required to be taken relating to privacy and data protection;

j. either of his own motion or upon request, report to the Minister as the need arises on any matter affecting the privacy of a data subject, including any recommendations relating to the need for or the desirability of, taking legislative, administrative or other action to give protection, or better protection, to the privacy of the data subject;

k. collaborate with supervisory authorities of other countries to the extent necessary for the performance of his duties, in particular by exchanging all useful information, in accordance with any convention to which [Name of Member State] is a party or any other international obligation of [Name of Member State] ;

l. generally monitor compliance by governmental and non-governmental bodies with the provisions of this Act;

m. prepare and issue or approve, in consultation with the industry stakeholders, appropriate codes of practice or guidelines for the guidance of business persons and institutions handling personal data;

n. undertake research into and monitor developments in data processing and information technology to ensure that any adverse effects of such developments on the privacy of data subjects are minimized, and include the results of such research and monitoring, if any, in the annual report required pursuant to section 72;

o. provide advice, with or without request, to a Minister or a public authority on any matter relevant to the operation of this Act and report to the Minister as the need arises on the desirability of the acceptance by [Name of Member State] of any international instrument relating to the privacy of data subjects;

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

q. exercise and perform such other functions as are conferred or imposed on the Data Commissioner by or under this Act, or any other enactment.

Confidentiality and Oath

56. (1) The Data Commissioner and every authorized officer shall take the oath specified in the Schedule before the Head of State.

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

a. in accordance with this Act or any other enactment; or

b. as authorized by the order of a Court

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

Powers of Commissioner

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

Power of Commissioner to Obtain information

58. (1) The Data Commissioner may, by a written information notice served on any person, request that person to furnish to him in writing in the time specified-

a. access to personal data;

b. information about and documentation of the processing of personal data;

c. information related to the security of processing of personal data; and

d. any other information in relation to matters specified in the notice as is necessary or expedient for the performance by the Data Commissioner of his functions and exercise of his powers and duties under this Act.

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

(3) A law in force in [Name of Member State] or rule of law prohibiting or restricting the disclosure of information shall not preclude a person from furnishing to the Data Commissioner any information that is necessary or expedient for the performance by the Data Commissioner of his functions.

(4) Subsection (3) shall not apply to information that in the opinion of the Minister responsible for national security is, or at any time was, kept for the purpose of safeguarding the security of [Name of Member State] or information that is privileged from disclosure in proceedings in any court.

Contents of Information Notice

59. The information notice specified in section 58 shall state-

a. that the person to whom the notice is addressed has a right of appeal under section [81] against the requirement specified in the notice within thirty days; and

b. the time for compliance with a requirement specified in the information notice, which time shall not be expressed to expire before the end of the period of thirty days specified in paragraph (a).

Failure or Refusal to Comply with Information Notice

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

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

(3) A person who contravenes subsection (1) or (2) commits an offence and is liable [on summary conviction] to a fine not exceeding […] dollars or to imprisonment for a term not exceeding […] months or to both.

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

Insufficient Information Pursuant to the Information Notice

61. If the Data Commissioner cannot, pursuant to a request under section 58(1), obtain sufficient information in order to conclude that the processing of personal data is lawful, the Data Commissioner may prohibit the Data Controller from processing personal data in any other manner than by storing the personal data.

Complaints to Commissioner and Powers of Investigation

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

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

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

b. as soon as reasonably practicable, notify the data subject concerned in writing of his decision in relation to the complaint and that the data subject may, if aggrieved by the Data Commissioner's decision, appeal against the decision to the Court under section [81].

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

Form of Complaint

63. (1) A complaint pursuant to this Act shall be made to the Data Commissioner in writing unless the Data Commissioner authorizes otherwise.

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

Notice of Investigation

64. Before commencing an investigation of a complaint pursuant to this Act, the Data Commissioner shall notify, in the case of a public authority, the Permanent Secretary and in any other case, the Chief Executive Officer, of the intention to carry out the investigation and shall include in the notification the substance of the complaint.

Powers of Entry Search and Seizure

65. (1) Subject to subsection (2), an authorized officer who is accompanied by a police officer may, at any time, enter the premises, to search them, to inspect, examine, operate and test any equipment found there which is used or intended to be used for the processing of personal data and to inspect and seize any documents, equipment or other material found there.

(2) An authorized officer shall not enter any premises to search and seize unless he is accompanied by a police officer and shows to the owner or occupier of the premises, a warrant issued by a [Magistrate or relevant authority (depending on jurisdiction)].

Matters Exempt from Inspection and Seizure

66. (1) The powers of inspection and seizure conferred by a warrant are not exercisable in respect of personal data which by virtue of Part V is exempt from any of the provisions of this Act.

(2) The powers of inspection and seizure conferred by a warrant are not exercisable in respect of -

a. any communication between a professional legal adviser and his client in connection with the giving of legal advice to the client with respect to his obligations, liabilities or rights under this Act; or

b. any communications between a professional legal adviser and his client, or between such an adviser or his client and any other person, made in connection with or in contemplation of proceedings under or arising out of this Act.

Power of Commissioner to Issue Enforcement Notice

67. Where the Data Commissioner is of the opinion that the Data Controller has contravened or is contravening a provision of this Act, the Data Commissioner may, subject to section 69, serve an enforcement notice on the data the Data Controller, requiring the data the Data Controller person to take such steps as are specified in the enforcement notice within such time as may be so specified to comply with the provision concerned.

Enforcement Notice

68. (1) An enforcement notice shall be in writing and shall-

a. specify the provision of this Act that, in the opinion of the Data Commissioner, the Data Controller has contravened or is contravening and the reasons for the Data Commissioner having formed that opinion; and

b. specify the action which the Data Commissioner requires the Data Controller to take;

c. subject to subsection (2), inform the Data Controller of his right of appeal pursuant to section [81] and the time within which the appeal must be lodged.

(2) An enforcement notice may, without prejudice to the generality of subsection (1), require the Data Controller-

a. to rectify or erase any of the data concerned; or

b. to supplement the personal data with such statement relating to the matters dealt with by them as the Data Commissioner may approve; and with respect to the personal data that is inaccurate or not kept up to date.

(3) The time specified in an enforcement notice for compliance with a requirement specified in the enforcement notice shall not be expressed to expire before the end of the period for appeal specified in section [81]

(4) On compliance by the Data Controller with a requirement under subsection (2), the Data Controller shall, as soon as may be and in any event not more than thirty days after such compliance, notify -

a. the data subject concerned; and

b. any person, where the Data Commissioner considers it reasonably practicable to do so, to whom the data were disclosed immediately before such compliance, of the rectification, erasure or statement concerned, if such compliance materially modifies the data concerned.

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

Failure to Comply with Enforcement Notice of an Offence

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

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

Investigations in Private

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

(2) In the course of an investigation of a complaint under this Act by the Data Commissioner, the person who made the complaint, head of the Data Controller or other relevant party shall be given an opportunity to make representations to the Data Commissioner, but no one is entitled as of right to be present during, to have access to, or to comment on, representations made to the Data Commissioner by any other person.

Referral to Commissioner of Police

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

Annual Report

72. The Data Commissioner is required to lay an annual report of the activities of his office in Parliament within […] months of the end of each financial year.

PART VIII – CONTRAVENTION AND ENFORCEMENT

Person Acting as a the Data Controller Without Registration

73. (1) A person who collects, processes or discloses personal information without first being entered into the register of the Data Commissioner, or outside of an approved agreement on behalf of a registered Data Controller, commits an offence under this Act is liable upon summary conviction, to a fine of not more than […] and to imprisonment for a term of […].

(2) where a jurisdiction believes it necessary to distinguish “sensitive personal information” it may include more punitive penalties than that outlined in (1) above for inappropriate collection, processing or disclosure of such information.

Breach of the Restriction of Transfer to Third Party Jurisdictions

74. (1) A person who is registered as a Data Controller under this Act who fails to adhere to any provision of section 19 commits an offence under this Act is liable upon—

a. summary conviction, to a fine of not more than […] or to imprisonment for a term of […]; and

b. conviction on indictment, to a fine of not more than [...] or to imprisonment for a term of not more than [...].

Obstruction of Authorized Officer

75. (1) A person shall not, in relation to the exercise of powers conferred by sections [66] and [67]-

a. obstruct or impede an authorized officer in the exercise of any of the authorized officer’s powers;

b. fail to provide assistance or information requested by the authorized officer;

c. refuse to allow an authorized officer to enter any premises in the exercise of the authorized officer’s functions;

d. give to an authorized officer any information which is false and misleading in a material respect.

(2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine not exceeding […] dollars, to imprisonment for a term not exceeding […] months or to both.

False Representations by Applicants

76. (1) A person who makes a request for access to or correction of personal information under false pretences commits an offence under this Act and is liable upon summary conviction, to a fine of not more than […] or to imprisonment for a term of […];

(2) A person who wilfully makes a false statement to mislead or attempts to mislead the Data Commissioner in the performance of his functions under this Act, commits an offence under this Act and is liable upon summary conviction, to a fine of not more than […] or to imprisonment for a term of […];

Breach of Confidentiality

77. A person who breaches the confidentiality obligations established by section [57], commits an offence under this Act is liable upon summary conviction, to a fine of not more than […] or to imprisonment for a term of […];

PART IX – MISCELLANEOUS

Whistle-blower Protection

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

a. the employee acting in good faith, and on the basis of reasonable belief has—
   i. notified the Data Commissioner that the employer or any other person has contravened or is about to contravene this Act;
   ii. done or stated the intention of doing anything that is required to be done in order to avoid having any person contravene this Act; or
   iii. refused to do or stated the intention of refusing to do anything that is in contravention of this Act; or

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

Fees

79. (1) The Minister may, pursuant to consultation with the Designated Authority, by regulation -

a. prescribe the fee to be charged by a data controller or category of data controllers for the making of a request by a data subject for their personal information

b. prescribe the manner in which any fee payable under this Act is to be calculated and the maximum amount it shall not exceed.

Regulations

80. (1) The Minister may, in consultation with the Data Commissioner, make Regulations for giving effect to the purposes of this Act and for prescribing anything required or authorised by this Act to be prescribed.

(2) Notwithstanding the generality of subsection (1), regulations made under this section may prescribe -

a. prescribing fees to be paid to the Data Controller;

b. providing procedural guidelines for appealing the decision of a Data Controller;

c. prescribing anything required to be prescribed under this Act; and

d. giving effect to the provisions of this Act.

(3) Regulations made under this section shall be subject to affirmative resolution of Parliament.

Role of the Courts

81. (1) Subject to subsection (2), an appeal lies to the Court against -

a. a requirement specified in an enforcement notice or an information notice;

b. a decision of the Data Commissioner in relation to a complaint; or

c. any decision of the Data Commissioner in respect of the performance of his duties and powers under this Act.

(2) An appeal shall be brought within […] days from the service on the person concerned of the relevant notice, or, as the case may be, the receipt by such person of the notification of the relevant refusal or decision.

(3) The Court shall have jurisdiction to hear and determine upon application by the Data Commissioner cases involving any contravention of the provisions of this Act and make appropriate Orders in relation thereto.

Section III:
Explanatory Notes to Model Legislative Text on Privacy and Data Protection

INTRODUCTION

1. This Model Privacy and Data Protection Legislative Text has been prepared as part of a set of Model Legislative Texts to enable the "Information Society" under a region-wide project that embraces CARICOM countries and the Dominican Republic.
2. The Information society is based on the premise of utilising automated processing systems to enhance service delivery to markets and persons anywhere in the world. In this new paradigm, considering the processing power of information systems, the opportunity for the abuse of information collected about a person in the course of a transaction has increased exponentially. Encouraging the use of these systems by the general public requires the establishment of systems that engender trust by the user and furnish comfort that information gathered will not be used in an unwarranted manner without sanction.
3. The Privacy and Data Protection framework is a key aspect of that larger system of trust-making.
4. The HIPCAR Model Legislative Text on Privacy and Data Protection is based on the Policy Building Blocks developed within earlier phases of the HIPCAR Project[4]. These Building Blocks reviewed international best practice of the objectives, key common tools and precedents, and identified the major policy positions and systems that need to be enshrined within legislative frameworks across the region[5]. The Model Legislative Text attempts to encode the policy guidelines into a legislative tool which attempts to balance the competing impetus of clarity of intent, structure and function and the necessary need for abstraction to facilitate its ready adaptation, as necessary, into the legislative framework of each HIPCAR Beneficiary State.
5. This Model Privacy and Data Protection Legislative Text comprises of nine parts, and eighty-one sections.

- **Part one** treats with preliminary considerations such as the short title, interpretation of particular terms in the model text and treats with concerns of the scope of applicability of the model text, as well as defines the general privacy principles which the model text enshrines.
- **Part two** treats with establishing a general obligation of public authorities and private bodies which can be deemed data controllers to undertake particular responsibilities with regard to the management of personal information in their control.

---

4 Ed.: The full title of the HIPCAR project is *"Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures".* This 3-year project was launched in September 2008, within the context of an umbrella project embracing the ACP countries funded by the European Union and the International Telecommunication Union. The project is implemented by the International Telecommunication Union (ITU) in collaboration with the Caribbean Community (CARICOM) Secretariat and the Caribbean Telecommunications Union (CTU).

5 Ed.: See also Chapter 1.5 of this document explaining the methodology. The Members of HIPCAR Working Groups include Ministry and Regulator representatives nominated by their national governments, relevant regional bodies and observers – such as operators and other interested stakeholders. The Terms of Reference for the Working Groups are available at www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/docs/ToR%20HIPCAR%20WGs.pdf.

- **Part three** creates the general right of individuals or data subjects to access, and be assured of the correctness of, their personal information retained by public and private bodies and creates the mechanism and procedures to facilitate the grant of such access.
- **Part four** identifies particular obligation of public authorities under the Model text. Such obligations are geared to the particular operational circumstances of public bodies.
- **Part five** treats with special conditions where the data controller's obligations to secure prior consent of the data subject for disclosure is not required.
- **Part six** treats with the procedures through which a data subject can seek a review of decision of a data controller to not provide access, and where necessary, further seek an appeal of the decision by an independent oversight body.
- **Part seven** provides the general framework and powers of the body designated at the oversight authority to monitor implementation of Privacy and Data Protection and provides a forum for appeals pursuant to the provisions of Part six.
- **Part eight** outlines particular offences to the provisions of the Model Text and the penalties associated with such offences.
- **Part nine** provides for miscellaneous considerations, including clarifying the role of the Courts, the establishment of a co-regulatory approach in the implementation of the oversight framework and establishes the powers to create regulations pursuant to the model text.

OVERVIEW OF CLAUSES

PART I – PRELIMINARY CLAUSES

6. **Part 1 of the Model Legislative Text (Act)** comprises of seven sections. The first sections provides for the preliminary clauses, including the short title and commencement provisions for the Law[6], as well as the general objective of the Law, to provide interpretive context to the sections thereafter presented.

Section 3: Interpretations and Definitions

7. Section 3 provides for the interpretation of particular terms in the Law[7]. Of interest are the interpretations for terms such as those outlined below.
8. "data" and "information"(terms which are made equivalent) underscore a wide interpretation of applicable forms, formats and technologies (electronic or otherwise) in which the data can be presented or stored. This is imperative as, notwithstanding the prevailing rationale associated with the ubiquity of information and communication technology (ICT), it provides for applicability of the Law and its intent in environments which may not be using ICT systems[8].
9. "data controller," the definition of which is intended to have broad catchment of the term "persons", including parties in both the public and private sectors. It is notable that the

[6] Ed.: The author of the Explanatory Notes mainly uses the notion "Law" when referring to the Model Legislative Text (Act) on Privacy and Data Protection.

[7] Policy Building Block 1.1 "There is a clear legal mandate in law to support the establishment of a regime to ensure the protection of personal and/ or private information."

[8] Policy Building Block 1.2 "The regime of data protection should not be technology specific, and should therefore have equal relevance in the paper-based or ICT-enabled environments".

definition does not suggest that all public or private sector agencies are data controllers, limiting the applicability of the Law to those persons who hold legitimate needs to treat with personal information in the course of their substantive business.[9]

10. Despite the Policy Building Blocks and some international precedent suggested the requirement for a distinction between "personal information" and "sensitive personal information" it was largely found that the relevant provisions were largely equivalent regarding the treatment of the two. As such, the Model Legislative Text provides for the subsuming of the definition of the latter into the former. Sensitive personal information was largely included into Data Protection frameworks as an additional means of treating with issues of sexual, racial or other types of unsavoury discrimination. This is generally achieved by further limiting the applicable processing of such traits (gender, sexual orientation, political views, ethnicity or race) beyond the general limitation otherwise provided for in the legislative framework, as well as providing enhanced penalties for breaches associated with this subset of information compared to those applicable to "non-sensitive" information. Despite this, there seems general consensus that Data Protection may not be the best locus for such provision. However, guidance is provided throughout the legislative text as to what areas may need further distinction if the jurisdiction decides to make the distinction between personal and sensitive personal information.[10]

11. "health care professional" and "health care institution" are terms which need appropriate definition as they form a recurrent basis for non-applicability or the law as it related to data subject consent to the collection, processing and disclosure of personal information. This exemption, like that which pertains to law enforcement, is based on ensuring that the data protection framework does not hamper the natural operation of such services. Generally, in the provision of health care, due to the specialist nature of the profession, it may be unreasonable to expect that the presiding practitioner will be able to identify all the parties to whom medical information will be shared in the determination of a diagnosis, or more critically, in the instance of emergency situations where the data subject may be incapacitated. Therefore, there needs to be a general exemption of these persons operating in these specific environment from the data protection framework, as this sector should be treated with specifically in more directly targeted legislation. It is notable that certain administrative functions not directly related to the provision of health care services should fall under the rubric of this exemption.

Section 4: The Act to Bind the State

12. Section 4 establishes that the Act binds the State. This provision is necessary as the Interpretation Acts of Member States express the well established rule of construction pronounced in the case of ***Attorney General v. Hancock [1940] 1 KB 427*** that an enactment does not bind or affect the right of the State unless it is expressly stated in the Act.[11]

Section 5: The Applicable Jurisdiction of the Act

13. Recognising the multi-national nature of certain business enterprises, and the globalised environment of commerce facilitated through the use of ICT, Section 5 attempts to provide clarity on the jurisdictional limits of the Law, with regard to data controllers which may be established in the particular jurisdiction (where the applicability is certain) and data controllers which may not be established or resident in the jurisdiction but which utilises resources therein located. This section is particularly important in the context of the provisions of Section 22.

9 Policy Building Block 1.4 "The law/ legal mandate should ensure that the obligation of privacy protection is applied by both Public and Private Sectors"

10 Policy Building Block 1.9 "The law/ legal mandate should identify a category of personal information as "sensitive information", requiring more stringent oversight and control."

11 Policy Building Block 1.3 "The law/legal mandate should clearly state that the law binds the State"

Section 6: Limiting the Applicability of the Act

14. Further Section 6 limits the applicability of the Law in respect of limiting information available by law to tribunals and the Courts.

Section 7: Overview of the Privacy Principles

15. This Part also outlines, in section 7, the privacy principles which the Act seeks to enshrine in the execution of public and private sector enterprises[12]. These principles, based on OECD and EU precedent include:

Accountability Principle

A data controller should be accountable for complying with measures which give effect to the principles stated above.

Collection Limitation Principle

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject[13.]

Data Quality Principle

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and up-to-date.

Purpose Specification Principle

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose[14.]

Use Limitation Principle

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

(a) with the consent of the data subject; or

(b) by the authority of law.

Security Safeguards Principle

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

Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller should be readily available.

Individual Participation Principle

An individual should have the right:

(a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

(b) to have communicated to him, data relating to him • within a reasonable time; • at a charge, if any, that is not excessive;

12 Policy Building Block 2.1 "Key Principles of the Data Protection framework are clearly defined in the [Law]"

13 Policy Building Block 1.7 "The law legal mandate clearly provides that personal information should be collected and processed with the consent of the subject of the personal information."

14 Policy Building Block 2.2 "Among the Key Principles of Data Protection shall be such provisions to ensure that at the time of collection the data subject is made of aware of the purpose/ use of such data and clearly consents to such purpose/ use of said data."

- in a reasonable manner; and
- in a form that is readily intelligible to him;

(c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

(d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended[15].

PART II – GENERAL OBLIGATIONS OF DATA CONTROLLERS

16. **Part 2 of the Model Law** outlines rules to which all data controllers must adhere in implementing the privacy principles outlined in Part 1.

Section 8: Registration of Data Controllers

17. Section 8 provides for the registration of data controllers and for the maintenance of a Register by the Data Commissioner. Alternatively, where the preference would be for a less obstructive notification process, such may be facilitated here[16]. In either case, this will allow compliance with the ***OECD Accountability and Openness Principles*** which requires that there should be a general policy of openness about developments, practices and policies with respect to personal data and resources regarding establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller should be readily available. Similarly, paragraph 8 (2) ensures compliance to ***OECD's The Collection Limitation Principle*** provides that there should be limits to the collection of personal data, that any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.[17,18] It is necessary to reiterate that the individual must know the purpose of the collection, use, disclosure, and must know that he or she can give or withhold consent. Express consent (communicated verbally or in writing) would generally be required but consent may be implied in limited circumstances. Consent must also be voluntary, must relate to the information in question, and may not be obtained by deception or coercion. Consent may also be withdrawn or limited by the individual giving the consent, in every case where consent (implied or express) is required.

Section 9: Limitation of Personal Information to Be Collected

18. These latter obligations associated with this Principle are included through Section 9, in conjunction with the stipulation that, where possible, the information should always be obtained from the data subject directly. Pursuant to this section, data controllers must ensure they can articulate the purpose for which personal data is being collected and the names of the person who are the intended recipients of the personal data. Despite these general rights, Section 9 (2) outlines particular circumstances where it may not be practical for the agency collecting the personal information to do so directly from the data subject.[19]

---

15 Policy Building Block 2.3 "Among the Key Principles of Data Protection should be such provisions to place the responsibility on the person and/or entity collecting and/ or processing the personal information of the security, accuracy and appropriate usage of that information."

16 Policy Building Block 3.1 "The law/ legal mandate shall clearly stipulate that there be provisions for the clear identification of collectors, users and processors of personal information such provision may include notification to or registration with the designated person."

17 Policy Building Block 4.1 "the law/ legal mandate shall reinforce that public authorities only collect personal information that is expressly authorised in law"

18 Policy Building Block 4.3 "The law/ legal mandate shall provide for the data subject to explicitly consent to the collection of information."

19 Policy Building Block 1.8 "The law/ legal mandate clearly specifies the circumstances under which personal information can be collected and processed without the consent or notification of the subject of the personal information."

Section 10: Purpose of Information Collection to Be Specified

19. Sections 10 establishes a framework to ensure compliance with the ***OECD Purpose Specification Principle***, whereby the purposes for which personal data are collected should be specified no later than at the time of data collection. As such, the data subject can determine whether he or she consents to the collection of that information as necessary to meet this purpose. Further, the data controller is therefore obliged to destroy personal data when it is no longer required. To achieve this end, data controllers must implement appropriate record management practices, including methods of secure storage and disposal.

Section 11: Limitation on the Retention of Personal Information

20. Section 11 therefore establishes limitations on the retention of such information only as long as is necessary for the fulfilment of the purpose for which it was collected, and other obligations (pursuant to Section 13 of this Law and others) where the data subject has a right to access the information.

Section 12: Appropriate Disposal of Personal Information

21. Pursuant to this definition of retention considerations, Section 12 similarly provides for the definition of appropriate disposal of information in accordance with best practices in records management. To provide for appropriate consultation (and flexibility) of the appropriate period that may be applied in conjunction with wider stakeholders (including, in the case of public records the National Archives of a jurisdiction), the final determination of this latter period is deferred to supporting Regulations to the principal law.

Section 13: Accuracy of Personal Information

22. Section 13 of the Model Law provides for compliance with the ***OECD Data Quality Principle***. This Section, in conjunction with Section 28 of Part 3, provides a framework whereby data controllers are responsible for the accuracy of the information retained or intended to be used for processing.

Section 14: Securing of Personal Information

23. Section 14 of the Model Law provides for compliance with the ***OECD Security Safeguards Principle*** which provides for personal data to be protected by reasonable security safeguards against such risks as:

    a) loss or

    b) unauthorized access,
       - i. destruction,
       - ii. use,
       - iii. modification, or
       - iv. disclosure

    of data. The security safeguards must be appropriate to the sensitivity level of the personal information. As such, the provision does not seek to prescribe a particular type of information security on the data controller. Appropriate oversight of adherence to guidelines, codes, and in the case of public authorities, approved risk assessments will facilitate the flexibility needed by the designated agency.

Section 15: Limitation of Use of Personal Information

24. Section 15 provides for compliance with the ***OECD Use Limitation Principle*** that personal data should not be processed for purposes other than those specified in accordance with the ***Purpose Specification Principle*** discussed above, as consent is required generally for any collection, use and disclosure of personal data[20]. It is noted that although the drafting provides for a data controller obtaining authorisation from the data subject subsequent to collection, this practice should be discouraged. Data controllers are required to provide data subjects with knowledge about and control over their personal data without interfering with the lawful and appropriate exchanges of information that are required to provide and support electronic commerce. Notwithstanding this general principle, there are instances where the information collected will need to be processed for other purposes or disclosed to other specified parties for the public good. To ensure that the provision is not substantially undermined, the exemptions are to be defined in the Law. Situations where processing of personal information qualify as exemptions from the general ***Use Limitation Principle*** are outlined in **Part V**.

25. It is noted that subsection (4) provides for the identification of different treatment for "sensitive personal information" as opposed to "personal information". Examples of how this can be implemented can be gleaned from EU jurisdictions, where data controllers are explicitly forbidden from processing sensitive personal information with prescribed exemptions[21], whereas personal information can be processed once that processing is consistent with the purpose for which it was originally collected, in accordance with the provisions of 15. Accordingly, in accordance with the ***Collection Limitation Principle***, it stands to reason that, except for the instances of identified exempt conditions, sensitive personal information should not be collected. Notable exemptions to this restriction of (collection and) processing, which are further limited than that provided for personal information, include:

    a) use by a health care professional in the particular circumstances of performance of medical and health related duties at a health care institution;

    b) use by law enforcement and security personnel in the express remit of crime prevention, suppression or detection, or other matters of national security;

    c) use in determining eligibility to a specified social service for which that information is necessary.

26. Section 16, 17 and 18 outline where personal information can be disclosed without prior consent of the data subject. These situations include those as listed below.

Section 16: Disclosure of Personal Information in Accordance with Purpose Collected

27. Section 16 provides for the disclosure of personal information for purposes that are consistent with the purpose for which collection and processing were consented to by the data subject, except for information collected in accordance with a written law, law enforcement actions, legal proceedings, or for the benefit of public health[22].

---

20 Policy Building Block 5.1 "The law/ legal mandate limits the collecting party from the use or processing of information to the purpose specified and consented to by the data subject at the point of collection"

21 Policy Building Block 5.9 "The law/ legal mandate prohibits the processing of sensitive personal information, except for specified instances and purposes…"

22 Policy Building Block 6.2 "The law/ legal mandate provides for the exemption of the obligation of consent of the data subject where required by a rule of law, if related to concerns of national security, provision of justice and health management."

Section 17: Disclosure of Personal Information for Research and Statistics

28. Section 17 provides for the disclosure of personal information for the undertaking of research and statistical analysis, where the data controller is assured that the security requirements are maintained and that the receiving party intends to comply with the provision of the Law.

Section 18: Disclosure of Personal Information for Archival Purposes

29. Section 18 provides for disclosure of personal information for archival purposes, where the information meets particular criteria, or where the data subject is deceased for a specified period. This clause essentially omits personal information relating to a person who is dead, but considered of national or otherwise cultural import which has been submitted to Archival institutions and bodies from falling under the ambit of the obligations of this model law. Without a similar clause the Law would prohibit the operation of bodies, such as the National Archives, which have considerable import in the preservation of national culture and history.

Section 19: Limitation of Inter-jurisdictional Transfer of Personal Information

30. Notably, with regard to the storage of personal information, Section 19 of this Part limits data controllers to undertaking such activity in either the jurisdiction where the Law is enforced or a jurisdiction with equivalent privacy protection laws. Where the latter situation applies, the data controller is obliged to first seek approval from:

    a) the Data Commissioner; and

    b) the data subject

    to effect the transfer. The data controller must proffer to the affected individual(s) the identity of the administrator of the privacy protection laws in the other jurisdiction[23]. A transitionary provision is included in subsection (5) in recognition that there are some trans-regional enterprises which may have arranged their businesses around data hubs within the region, and also recognising that implementation of such a provision as Section 19 is not reasonably expected to be simultaneous across the region. In this way, the Data Commissioner may prescribe some reasonable period by which data hubs are migrated to appropriately protected jurisdictions before any sanction is imposed.

31. Sections 20 and 21 of this Part provides for the Data Commissioner's utilising a co-regulatory approach where such is deemed appropriate, so as to best balance the regulatory imperatives of its function while minimising the impact and cost on industry.

Section 20: Establishment of the Codes of Conduct

32. Section 20 provides for the development of sector-specific Codes of Conduct. These Codes of Conduct, be them voluntary or mandatory, are deemed to be key to the furtherance of the private sector adhering to the general privacy principles outlined in Part 1. Further, subsection (2) provides that the Data Commissioner may petition to sector or industry regulators, where such have been established, in the development of these Codes of Conduct.

[23] Policy Building Block 6.3 "The law/ legal mandate limits the trans-border transfer of personal information to jurisdictions without comparable privacy and data protection laws and systems. In such instance, the law provides for a transfer of information only as much as will not result in a compromise of the protection of the data subject's information"
Policy Building Block 6.4 "The law/ legal mandate provides, notwithstanding any standards restriction, that the transfer of personal information may be facilitated with the express consent of the data subject to transfer the information to that jurisdiction, pursuant to the data subject being notified of the attendant risks.

Section 21: Mandatory Codes of Conduct

33. The Part provides that, where Codes of Conduct are deemed mandatory, the Minister may establish these Codes as Regulations, subject to affirmative resolution of Parliament.

PART III – RIGHTS OF THE DATA SUBJECT

34. **Part 3 of the Model Law** treats with the rights of the data subject with respect to access to personal information held by a data controller. The ***OECD Individual Participation Principle*** makes provision for an individual to have the right to obtain from a data controller confirmation of whether or not the data controller has data relating to him; access to that information and the opportunity to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Section 22: Right of Individual to Access Own Personal Information

35. Legislation and case law usually provide for an individual to have full access to his own personal records with very limited exceptions, and it is appropriate that privacy legislation would continue this right, which is generally provided by the provisions of Section 22[24]. However, there are specific details that require further consideration. The right to access to personal data is not absolute, as there may be some limited exceptions to this right.

Section 23: Data Controller May Refuse Access

36. Section 23 provides the framework under which a data controller may refuse access to an applying individual, while ensuring that if the access is so denied, to all or part of a document, the onus falls on the data controller to justify the denial. These exceptions include, for example, instances where a request for access is denied so as to protect the individual or another person[25], or alternatively, due to established considerations of information protection, such as where the information is subject to legal privilege (e.g. solicitor-client privilege), or where information was collected in the course of an investigation or primarily for use in a legal proceeding.
37. Further, while it is expected that the vast majority of individuals would request their information in a responsible manner, there is also reasonable anticipation that occasionally there would be individuals who request their information for no reason except to obstruct the operations of a data controller. For example, a data subject could make weekly requests for information, even though the information has been provided and has not been updated. In these cases, it may be appropriate to allow the data controller to refuse the request. As is the case with most refusals of a right, the onus would be on the data controller to justify the refusal. Section 23 (2) provides for this eventuality and provides the data controller with the basis for such a refusal.

Section 24: Severance of Exempt Information

38. Section 24 undertakes to provide guidance to the Data Controller on the appropriate course of action where a response to a request for access may result in disclosure of the personal information of another individual. Where possible, it is proposed that the information that would cause such undesired associated disclosure be redacted before the release of the information requested.

---

24 Policy Building Block 6.5 "The law/ legal mandate provides for the disclosure of personal information in response to a request from the data subject. Where disclosure may result in the disclosure of other restricted information, the law/ legal mandate shall prescribe the appropriate guidance to the Head of the processing party."

25 Policy Building Block 6.5 "*sic*."

39. Subsection (2) clarifies that the obligation of the Data Controller to protect the personal information of others extends to even the limiting of the acknowledgement that certain information exists.

Section 25: Data Subject May Delegate Rights to Third Party

40. Section 25 provides for the delegation of particular rights of a data subject to another person. The principal right delegated in the context of this Law would be the right to consent to the collection, processing, or disclosure of personal information. This section provides that consent may be given by the individual or the individual's substitute decision-maker. In situations where a substitute decision-maker is required to act on an individual's behalf, such as where the data subject is below the age of majority, or where due to a health condition, the data subject is unavailable to consent (e.g. where the individual is out of State), or where the individual is deceased, the legislation provides a hierarchy of individuals, consistent with laws relating to parental responsibility, who would be asked to make information decisions on behalf of the individual.

Section 26: Time Limits for Response to Requests

41. Section 26 establishes a broad performance target which data controllers must meet with regard to responses to requests from data subjects. Among other things, such a performance benchmark shall encourage data controllers to establish and have in place a process to manage the receipt and response to such requests. Such a process may include the definition of standard procedures for data subjects to follow when requesting a copy of their personal data. This may include a form, a time during which the record will be provided, and a fee (if applicable).

Section 27: Correction of Errors in Stored Personal Information

42. Pursuant to the OECD Principle, another right to be made available to data subjects under privacy legislation includes the right to request a correction of information. Such is facilitated by Section 27. Such cases may arise where the correction a data subject wishes to make may be a factual error (e.g. wrong date of birth). While in such cases professional or other institutional standards would not always allow a record to be changed, the framework provides for the data controller to place a notation on the record that the personal information has been verified and to outline the correct information. The data controller may also place a statement of disagreement outlining the individual's disagreement with the information on the record.

PART IV – PARTICULAR OPERATIONAL OBLIGATIONS OF PUBLIC AUTHORITIES

43. **Part 4 of the Model Law** outlines particular rules to which the heads of public authorities must adhere in implementing the privacy principles outlined in Part 1, in conjunction with the general guidelines outlined in Part 2. These particular obligations are geared to ensure appropriate systems of controls are established in law to facilitate the monitoring of the implementation of the Privacy Principles.

Section 28: Privacy Impact Assessments

44. Notable examples of such systems include, in Section 28 of this Part, the obligation of public authorities to prepare Privacy Impact Assessments of existing or planned information processing operations in accordance with the guidelines of the Data Commissioner. These Impact Assessments may form the basis of a co-regulatory approach between the public authorities and the Data Commissioner that effects an *ex ante* approach to authorisation of processing functions. While this may cause some administrative delay in the establishment of new

processing system, this will have an overall benefit to the flexibility and responsiveness of the public authority compared to an *ex post*, or *ad hoc* approach to authorisation of processing functions.

Section 29: Personal Information Filing Systems

45. Section 29 provides a functional requirement of public authorities which, again, is structured to assist the Data Commissioner's work in ensuring compliance to the obligations of the Law. The statutory requirement to establish particular information filing systems in which all personal information under the control of the public authority is primarily stored and managed facilitates the effectiveness of such other mechanisms that may be implemented. Despite this general requirement, it must be recognised that the National Archives may manage personal information that is archival in nature.

Section 30: Exemption of National Archives from Section 29

46. Section 30 provides for the particular exemption of the National Archives from the provisions of section 29, as this information, authorised for public consumption through the National Archives, generally do not fall under the sphere of coverage envisaged by the establishment of personal information filing systems.

Section 31: Establishment of Liaisons Within the Data Controller

47. In line with the general approach of establishing particular functional requirements of public authorities to effect the oversight of Privacy Protection, Section 31 provides for public authorities to identify liaison officers within their organisations to facilitate the internal evaluation of systems and function in compliance with the Data Protection Law. In this way, operational benefits can be expected to accrue as public authorities will proactively structure their systems and processes to ensure compliance with the privacy principles and the privacy protection provisions in Law, as well as from improved channels of communication with the Office of the Data Commissioner. While this may seem appropriate to the operations of a public authority, such a provision may not be well-suited for some private enterprises, thus the establishment of this provision as a specific obligation of the public sector.

Section 32: Prior Authorisation Required for Information Sharing Agreements

48. Section 32 thereafter facilitates the sharing of information between Ministries in accordance with guidelines established by, and/or approval attained from the Data Commissioner. These are critical to the implementation of e-government service provision.

Section 33: Data Commissioner to Publish a Report on Information Filing Systems

49. Section 33 obliges the Commissioner to publish reports of the status of the various mechanisms and instruments established in this Part to monitor the management of personal information acquired by public authorities. This will facilitate the timely dissemination to the public of the information being held by a given public authority allowing individuals the visibility to utilise the provisions of Part 3 to exercise their rights to access information about them.

PART V – SPECIAL EXEMPTIONS

50. **Part 5 of the Model Law** provides general enabling provisions for the Minister to make amendments by Order to the applicability of provisions in Part 2 to identified groups of data controllers for specific purposes and circumstances. These clauses were modelled significantly on that enacted in the UK and Malta, based on the appropriate Directives of the European Commission.

Section 34: Personal or Family Use

51. Section 34 makes clear that a person may use personal information where that information is used for personal or family affairs.

Section 35: National Security, Crime or Taxation

52. Sections 35 provides for particular exemptions from Parts 2, 3 and 4 of the Law in accordance with international best practice. The exemptions are well-articulated in precedent with regard to the processing of personal data and on the free movement of such data when such a restriction constitutes a necessary measure to safeguard:

    (a) national security, defence; or public security;

    (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

    (c) an important economic or financial interest of a jurisdiction, including monetary, budgetary and taxation matters;

Section 36: Exemption of Regulatory Affairs

53. Section 36 provides for exemptions in the instance monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority, the protection of the data subject or of the rights and freedoms of others.

Section 37: Exceptions Relating to Journalism and the Arts.

54. Section 37 provides for exemption of applicability in relation to endeavours associated with the existing freedoms of expression, including in the pursuit of works in journalism, literature and art. This clause is based on similar clauses enacted in Data Protection frameworks in Europe. Adequate protection against defamation of character generally are already in place to provide some sort of protection to the data subject without the undue restriction of activity. Further, the section provided for the Commissioner to establish sectoral codes which may facilitate the appropriate balance of the objects of the Law and the prevailing right of freedom of expression.

PART VI – REVIEW AN APPEAL OF DECISIONS OF DATA CONTROLLERS WITH REGARD TO ACCESS

55. **Part 6 of the Model Law** provides for a data subject to appeal and/or seeks review of a decision of a data controller with the Data Commissioner[26]. This section is critical as it empowers the individual to force fair treatment from a data controller by way of an appeal through an independent authority.

Section 38: Right of a Data Subject to Appeal a Decision

56. Section 38 provides the general right of appeal of an individual who is dissatisfied by the outcome of a request made pursuant to sections 23 (right to access one's personal information) and section 28 (right to request a correction of one's personal information). This section provides for the appeal of the relevant decision to the Data Commissioner, who is empowered to resolve the dispute.

[26] Policy Building Block 5.8 "The law/ legal mandate provides for the appeal of decisions of the head of the processing party to the designated agency"

Section 39: Time Limit for the Data Subject to Lodge an Appeal

57. Sections 39 through 41 provide for the generic process by which an appeal is to be accepted by the Data Commissioner. Section 39 outlines the maximum timeframe from the time of the decision in question in which the appeal should be lodged, to ensure a speedy initiation of the process.

Section 40: The Data Commissioner May Dismiss an Appeal

58. Section 40 provides for the Data Commissioner to dismiss an appeal before notification to the head of the data controller if, in his opinion, the basis for the appeal is not substantial.

Section 41: The Data Commissioner to Inform the Data Controller

59. In accordance with standard procedure, Section 41 directs the Data Commissioner to issue a notice to the head of the Data Controller of a pending appeal related to a decision of the Data Controller.

60. Sections 42 through 46 provide the general mechanism through which the Data Commissioner may utilise alternative dispute resolution techniques in the resolution of the appeal.

Section 42: The Commissioner Appointing a Mediator or Acting as an Arbitrator

61. Under section 42, the Commissioner may appoint a mediator as a means for dispute resolution, until ultimately, action on behalf of the Commissioner himself as an arbiter.

Section 43: The Commissioner Conducting an Enquiry

62. Notably, Section 43 provides for the Data Commissioner to undertake an enquiry in response to an appeal where the decision rendered pursuant to that enquiry is to be binding on the parties.

63. Sections 44 through 46 provides for the procedural and operational conditions in which an enquiry will be undertaken.

Section 44: The Commissioner May Hold Enquiries in Private

64. Section 44 provides for the discretion of the Data Commissioner to hold such enquiries in private.

Section 45: Representation of parties at an enquiry

65. Section 45 provides for either party to be represented by counsel or other agents on their behalf at the enquiry.

Section 46: Burden of Proof at an Enquiry

66. Section 46 outlines the legal premise under which the enquiry would be heard, placing the burden of proof on the party deemed to have availability of more resources, the Data Controller.

Section 47: Recourse to the Courts to Appeal the Decision of an Enquiry

67. Section 47 provides for the Courts to be a forum of appeal of any decision made at the enquiry.

PART VII – ESTABLISHMENT, FUNCTIONS AND POWERS OF THE OVERSIGHT AUTHORITY, THE DATA COMMISSIONER

68. **Part 7 of the Model Law** establishes the Office of the Data Commissioner. This is a critical component of an effective privacy legislative framework. The requirement for independent

oversight is essential to oversee compliance by the data controllers, in both the public and private sectors. It should be noted that while this part is drafted as if the head of this body was an individual (thus the "Data Commissioner"), it is equally valid that this body is headed by a group of persons (thus a "Data Commission", "Data Tribunal" or the like). The jurisdictions retain ultimate discretion in the form of governance preferred for this oversight body. What is critical is that such a body is independent, from the Political Executive and that that there is sufficient autonomy from certain private sector interests that would fall under the rubric of this law by the nature of the business they undertake.

Section 48: Establishment of the Office of the Data Commissioner

69. In light of the scope of this function, to ensure privacy oversight remains untainted by perception of bias to any group of data controllers, Section 48 provides for the appointment and removal of an independent Data Protection Commissioner in the same manner as and with similar criteria for eligibility a Parliamentary Commissioner or Ombudsman[27], where the Commissioner may only be removed for cause.

70. In the instance of the absence of the Data Commissioner, the Section also provides for the temporary appointment of a Commissioner until a new incumbent is identified.

71. Alternatively, legislation can include provision for the appointment of a Deputy Data Commissioner, who will act on behalf of the Commissioner if the need arises. Further, the section ensures that the Commissioner has no other emolument income or other expressed obligation or allegiance which could engender the perception of bias[28]. This aspect of the clause may be amended in accordance with the governance model proposed and the logistical concerns in each jurisdiction. It is proposed in this Model Text primarily as the traditional regulatory function of the Executive towards the market must, in this case, also be applied to the public sector. However, as a group of data controllers may be public and quasi-public sector enterprises over which the Political Executive would retain some administrative oversight, the overall governance framework provides for:

    a) Reporting to the relevant Minister on the status of privacy protection by the private sector;

    b) Reporting to the Parliament on the status of privacy protection by public authorities.

72. This section also provides for, in subsection (3) the Data Commissioner hiring personnel in pursuance to the execution of the functions of the Office. Finally, this section defines a timeframe after the proclamation of the Law by which the Data Commissioner should be established.[29]

Section 49: Distinct Legal Identity of the Data Commissioner

73. In any case, Section 49 provides for the Commissioner to be charged with a distinct legal personality so that the Commissioner is capable of entering into contracts, acquiring, holding and disposing of any kind of property for the purposes of his functions, suing and being sued,

---

27 Policy Building Block 3.3 "The Head of the designated agency shall be appointed in a manner to ensure independence and impartiality of functions.

28 Policy Building Block 3.4 "The Head of the designated agency shall be afforded such terms and conditions of employment, including provisions of entrenchment and conditions of reappointment, included in the law/ legal mandate that are sufficient to limit the opportunity for inducement or coercion."

29 Policy Building Block 3.12 "The law/ legal mandate shall specify a timeframe in which the designated agency will come into force on the passage of the Law."

and doing all such things and entering into all such transactions as are incidental or conducive to the exercise or performance of his functions under the Law[30].

Section 50: Definition of Tenure of the Office Holder

74. Further, as a mechanism to maintain the integrity of the office and to provide for integrity and fairness, Section 50 establishes a maximum term of office for the Commissioner. This term is longer that the election cycle, having regard to best practice[31].

Section 51: Remuneration of the Data Commissioner and Staff

75. Further, in order to preserve the independence and impartiality of the Commissioner, Section 51 provides for the remuneration of the Commissioner and his staff to be determined through an independent means so that the Office holder would not seem to be beholden to any administration. The language selected here is utilised to provide the requisite flexibility for jurisdictions to determine the appropriate mechanism by which this independence is achieved. As an example, some jurisdictions will have the salaries of such independent offices determined by an independent Commission, or alternatively set by regulation. The proposed clause does not presume to dictate either mechanism as appropriate, but singly wishes to reinforce that once determined, the fiscal allocation should be transparently outlined in the annual government budgeting cycle under a separate heading of expenditure.

Section 52: Protection of the Data Commissioner

76. Further, in order to preserve the independence and impartiality of the Data Commissioner, Section 52 provides for protection of the Data Commissioner from liability in respect of an act committed or omitted in good faith in the exercise or purported exercise of his or her functions. That protection should not extend in cases of personal injury. Additionally, provision is made in the legislative framework to indemnify the Data Commissioner for the cost of defending actions[32].

Section 53: Delegation of Powers of the Data Commissioner

77. As a matter of operational and organisational practicality, Section 53 empowers the Commissioner to delegate any of his investigative and enforcement powers conferred upon him or her by this Law to any authorized officer designated for that purpose by the Commissioner[33].

Section 54: Independence of the Data Commissioner

78. Section 54 reinforces that the Commissioner is required to act independently in the exercise of his or her functions under the Law and is not to be subject to the direction or control of any other person or authority[34].

---

30 Policy Building Block 3.2 “The agency designated to ensure compliance with the law/ legal mandate shall be a distinct legal person with the power to own or dispose of assets, the ability to enter into contracts, and who shall independent in the performance of its functions.

31 Policy Building Block 3.4, *sic*

32 Policy Building Block 3.10 “In the law/ legal mandate, the designated agency may be provided protection from liability for any acts done in good faith in the exercise of its function.”

33 Policy Building Block 3.6 “The Head of the designated agency shall be afforded in the law/ legal mandate the power to delegate certain authority to recognised agents to facilitate the execution of his function.”

34 Policy Building Block 1.6 “The law/ legal mandate clearly provides for the independence of the designated agency.”

Section 55: Functions of the Data Commissioner

79. As outlined in Section 55, the major functions of the oversight body, an administrative office led by its head, the Data Commissioner, would be to ensure compliance with the privacy legislation through -

- monitoring how the legislation is administered and conducting reviews;
- initiating privacy compliance investigations;
- resolving and mediating privacy complaints;
- providing review and oversight impact assessments relating to privacy;
- undertaking research matters relating to privacy legislation;
- developing public education programs;
- promoting best practice with regard to privacy; and
- providing advice and comments to data controllers.

Section 56: Oath of Confidentiality

80. Section 56 requires that persons who, by virtue of the execution of functions under this Law, have access to information which can be considered private or personal, shall be required to take the oath not to divulge any data obtained as a result of the exercise of a power or in the performance of a duty under the Law except in accordance with this particular provisions of the Privacy Law, any other enactment, or as authorized by the order of a Court.

Section 57: General Powers of the Data Commissioner

81. Sections 57 renders the Commissioner as an entity akin to a regulator for the purpose of carrying out his or her functions, including the necessary power to do all such acts as appear to him or her to be requisite, advantageous or convenient for, or in connection with the execution of these functions, including the power to investigate the operations of a data controller[35], on his own initiation or in response to a complaint, to obtain information about documentation, processing and security of data, and , *inter alia*, to request that a person furnishes to him or her in writing in the time specified access to personal data, or other specified information relating to the information management practices of the controller[36].

82. Sections 58 through 61 establish a mechanism through which the Data Commissioner may request information pursuant to an investigation, the information notice, and reinforces the obligation by prescribing a failure to respond to or comply with an information notice by the Commissioner as an offence[37].

Section 58: Power of the Data Commissioner to Obtain Information From a Data Controller

83. Section 58 introduces the mechanism of preliminary interrogation or data gathering – the information notice. The section also outlined when the information notice is to be used, and the form in which such a notice can take in being served to the relevant party. In line with the

---

35 Policy Building Block 3.5 "The Head of the designated agency shall be afforded in the law/ legal mandate the necessary powers of investigation to facilitate the execution of functions of the Data Protection framework."

36 Policy Building Block 3.7 "The designated agency may undertake audits or investigations into persons to whom the framework is applicable, either on its own accord or in response to complaints from the public. The person who shall bear the cost of such investigations shall be determined in Regulations."

37 Policy Building Block 3.8 "Persons to whom the law applies shall cooperate with the designated agency in the exercise of its function, under the penalty of civil and/ or criminal penalties."

general consideration of the use of technologies to facilitate timely transmission, subsection (2) provides for the consideration of the form by information requested may be submitted.

84. Subsections (3) and (4) reinforce issues of exemption addressed earlier in the model text. These are inserted for the avoidance of doubt on the treatment of such issues.

Section 59: Content and Form of the Information Notice

85. Section 59 outlines the necessary contents of an information notice which, in essence, informs the party served of their rights to undertake a process to protect themselves in accordance with the framework of the model text.

Section 60: Establishing the Offence of Failing to Comply With an Information Notice

86. Section 60 outlines that failure to respond to an information notice is to be deemed a material breach of the Law and may subject the offending party to sanction and penalty under the provisions of the Law. Further, the subsection (3) outlines the reasonable defence to such a summary conviction.

Section 61: Recourse of the Data Commissioner to Insufficient Response to an Information Notice

87. Section 61 treats with how the Data Commissioner is to act in the instance that it is deemed that a response to an information request is not sufficient, including ordering the cessation of operations which treat with the collection, processing or disclosure of personal information.

88. Sections 62 through 66 establish the appropriate process by which the Data Commissioner may undertake an audit or investigation, including the receipt of a complaint from an individual, the subsequent notification to the data controller of a pending investigation, and the provision for the entry, search and seizure powers (subject to an issued warrant, and accompanied by a police officer).[38]

Section 62: Data Commissioner's Response on Receipt of a Complaint

89. Section 62 addresses the Data Commissioner's obligation to act in particular fashions on receipt of a complaint. These obligatory actions include undertaking an investigation and notifying the complainant of the outcome of that investigation in a reasonable time. Subsection (3) reinforces provisions earlier which treat with agents acting on behalf of an individual initiating this process.

Section 63: Form and Content of a Complaint

90. Section 63 outlines the general form to which a complaint must adhere once lodged by a complainant, and obliges the Commissioner to give such reasonable assistance as required to ensure that the form of complaint is appropriate. The Data Commissioner is not to assist in the substance of the complaint.

Section 64: Data Commissioner's Initiation of an Investigation Pursuant to a Complaint

91. Section 64 outlines the process the Data Commissioner must undertake in engaging the Data Controller subject to a complaint. The mechanism proposed – the Notice of Investigation – must be served on the head of the Data Controller prior to the commencement of an investigation.

---

[38] Policy Building Blocks 3.9 "The designated agency may make requests, to which persons must comply, for the submission of certain documents to facilitate its investigations. The agency may gain a warrant from the Courts to achieve such if it is [required]"

Section 65: General Power to Undertake Searches and Effect Seizures in the Course of an Investigation

92. Section 65 provides the Data Commissioner with the general authorisation to enter premises of a Data Controller, undertake a search, and where necessary, seize relevant documentation in the course of an investigation. Subsection (2) of this section limits the application of this general authorisation such that a warrant must first be obtained to this effect, and that the officers of the Data Commissioner should be accompanied by a police officer.

Section 66: Exemptions From Seizure

93. Section 66 reinforces that earlier provisions of particular documents being exempt from processing under this law are similarly applicable in the instance of search and seizure.

94. Once the investigation is complete, an instance may arise where the Data Commissioner is of the opinion that the Data Controller is not operating in alignment with the Privacy Protection obligations. In that instance, Sections 67 through 69 establish the mechanism and process by which the Data Commissioner may issue directions to data controllers deemed to be operating in a manner not consistent with the Law.

Section 67: The Enforcement Notice

95. Section 67 empowers the Data Commissioner to issue the mechanism proposed – the enforcement notice – and delineates the appropriate application of such and, for avoidance of doubt, limits the target of same, the Data Controller.

Section 68: Form and Content of the Enforcement Notice

96. Section 68 outlines the specific form of the enforcement notice, and enshrines into this mechanism the necessary binding authority to instruct the offending Data Controllers to act to rectify the determined breach. This section also provides for the mechanism, and the form of that mechanism, by which the Data Controller responds to the enforcement notice, and includes a maximum timeframe by which such a response is expected. In this way, Data Controllers are herein obliged to respond or comply with instructions within the enforcement notice.

Section 69: Establishing the Offence of Failing to Comply With an Enforcement Notice

97. Section 69 outlines that failure to treat with an enforcement notice as outlined in Section 68 would be deemed a material breach of the Law and exposes the Data Controller to criminal sanctions.[39]

Section 70: Conditions of the Investigation

98. Sections 70 establishes further logistical conditions within which the investigations should be held. Subsection (1) mandates that all investigations be conducted with an insistence on confidentiality.

99. Subsection (2) provides for the parties to each make representations to the Data Commissioner during the course of the investigations. However, it notes that at this stage of the investigation, the provision goes on to debar the presence of either party at the disposition of the other.

Section 71: Referral of Matters to the Commissioner of Police

100. Section 71 provides for the appropriate action of the Data Commissioner in the referral of the record to the appropriate person where a breach is deemed to have occurred.

[39] Policy Building Block 3.8 *sic*

101. Section 72: The Data Commissioner to Report Annually to the Legislature

102. Section 72 obliges the Data Commissioner to report on its activities to the Parliament, in line with Parliamentary best practice.[40]

PART VIII – ESTABLISHING OFFENCES AND PENALTIES FOR BREACH OF PROVISIONS

103. **Part 8 of the Model Law** outlines the criminal offences associated with the breach of particular provisions of the Law.

Section 73: Offence to Collect Personal Information Without Due Notice to the Subject

104. Section 73 deems the breach of section 8 as an offence. Where jurisdictions decide to make a distinction between sensitive and non-sensitive personal information, there is the option to provide for different penalties associated with this offence where the breach is deemed to have occurred with personal information and sensitive personal information respectively. Where such an approach is pursued, it is advisable that the penalty for the breach of the latter information type will be more punitive.

105. While the obligations enshrined in provisions 8 through 15 and 20 are all critical to the effective implementation of Data Protection, breaches of these may be adequate remedies without the imposition of criminal sanctions. However, it is suggested that due to the implications on international trade agreements, breaches of section 19 should be treated even more seriously than the others.

Section 74: Offence to Effect Extra-jurisdictional Transfer of Personal Information Without Proper Authorisation

106. Accordingly, Section 74 defines a breach of that particular provision 19 as a criminal offence, and provides for the definition of the standard penalty associated with such an offence[41].

Section 75: Offence to Obstruct an Agent of the Data Commissioner

107. Section 75 treats with the direct or indirect obstruction of authorised agents of the Data Commissioner in the exercise of their functions during an investigation and outlines the standard penalty associated with this offence.

Section 76: Offence to Make False Representation to the Data Commissioner or His Agents

108. Section 76 treats with persons who are deemed to have abused the rights conferred by Part 3 of the Law. The offences created and the penalties outlined are to be disincentives to the vexatious abuse of these empowering provisions which would otherwise undermine the operational viability of the data controller, the Office of the Data Commissioner or both.

Section 77: Offence to Breach the Oath of Confidentiality

109. Section 77 seeks to treat with persons who breach oaths of confidentiality entered into in undertaking functions within the Office of the Data Commissioner. This is geared to limit such occurrences and ensure the continued public trust in the Office.

---

[40] Policy Building Block 3.11 "The designated agency shall report annually to the Parliament/ Legislative Council on its operations for the year prior."

[41] Policy Building Block 5.10 [6.6] "The law/ legal mandate prescribes civil and criminal penalties for the breach of the defined provisions relating to the use or processing [disclosure] of personal information. Such penalties may be levied against the processing party, or any officer or director that can be proven to have breached the law/ legal mandate."

110. Breaches to the provisions of the Law which are not explicitly outlined either in this Part of other prevailing sections may be treated by the Courts under civil law.

PART IX – GENERAL PROVISIONS TO FACILITATE IMPLEMENTATION OF THE FRAMEWORK

111. **Part 9 of the Model Law** provides for miscellaneous considerations that will be beneficial to the enactment of the main aspects of the Law previously outlined in the preceding Sections.

Section 78: Whistleblower Protection

112. Section 78 provides protection for persons who, while within the employ of a Data Controller becomes knowledgeable of actions by that party which run counter to the objects of this Law or the provisions therein, wilfully informs the relevant authority of such action. This "whistleblower protection" provision is geared to bring comfort to employees to act in the interest of the public good by limiting any retributive action by the head of the data controller. The effect of this whistleblower provision is to increase the avenues through which information of malfeasance in privacy protection is reported to the authorities for speedy rectification and/or enforcement.

Section 79: Fees to Be Levied For Services of the Data Commissioner

113. Section 79 provides for the Minister, acting on the advice of the Data Commissioner, to establish a schedule of fees for the services rendered by that Office. This is to facilitate the recouping of some of the costs associated with the operation of the Office.

Section 80: Minister to Establish Necessary Regulations

114. Section 80 provides a general enabling provision through which the relevant Minister may enact Regulations necessary to effect or elaborate on particular provisions throughout the Law.

Section 81: Role of the Courts

115. Section 81 clarifies the role of the Courts as the ultimate appellate forum where either party remains dissatisfied with the outcome of any dispute resolution process undertaken by the Data Commissioner. This Section also reinforces the power of the Courts to impose civil penalties for breaches of the Law not deemed an offence by Part 8 of the Law.[42, 43, 44]

---

[42] Policy Building Block 4.8, *sic*

[43] Policy Building Block 5.10, *sic*

[44] Policy Building Block 6.6, *sic*

ANNEXES

Annex 1

Participants of the First Consultation Workshop for HIPCAR Project Working Group dealing with ICT Legislative Framework – Information Society Issues
Gros Islet, Saint Lucia, 8-12 March 2010

Officially Designated Participants and Observers

Country	Organization	Last Name	First Name
Antigua and Barbuda	Ministry of Information, Broadcasting, Telecommunications, Science & Technology	SAMUEL	Clement
Bahamas	Utilities Regulation & Competition Authority	DORSETT	Donavon
Barbados	Ministry of Finance, Investment, Telecommunications and Energy	BOURNE	Reginald
Barbados	Ministry of Trade, Industry and Commerce	COPPIN	Chesterfield
Barbados	Cable & Wireless (Barbados) Ltd.	MEDFORD	Glenda E.
Barbados	Ministry of Trade, Industry and Commerce	NICHOLLS	Anthony
Belize	Public Utilities Commission	SMITH	Kingsley
Grenada	National Telecommunications Regulatory Commission	FERGUSON	Ruggles
Grenada	National Telecommunications Regulatory Commission	ROBERTS	Vincent
Guyana	Public Utilities Commission	PERSAUD	Vidiahar
Guyana	Office of the Prime Minister	RAMOTAR	Alexei
Guyana	National Frequency Management Unit	SINGH	Valmikki
Jamaica	University of the West Indies	DUNN	Hopeton S.
Jamaica	LIME	SUTHERLAND CAMPBELL	Melesia
Saint Kitts and Nevis	Ministry of Information and Technology	BOWRIN	Pierre G.
Saint Kitts and Nevis	Ministry of the Attorney General, Justice and Legal Affairs	POWELL WILLIAMS	Tashna
Saint Kitts and Nevis	Ministry of Youth Empowerment, Sports, Information Technology, Telecommunications and Post	WHARTON	Wesley
Saint Lucia	Ministry of Communications, Works, Transport and Public Utilities	FELICIEN	Barrymore
Saint Lucia	Ministry of Communications, Works, Transport and Public Utilities	FLOOD	Michael R.
Saint Lucia	Ministry of Communications, Works, Transport and Public Utilities	JEAN	Allison A.
Saint Vincent and the Grenadines	Ministry of Telecommunications, Science, Technology and Industry	ALEXANDER	K. Andre
Saint Vincent and the Grenadines	Ministry of Telecommunications, Science, Technology and Industry	FRASER	Suenel

Country	Organization	Last Name	First Name
Suriname	Telecommunicatie Autoriteit Suriname/Telecommunication Authority Suriname	LETER	Meredith
Suriname	Ministry of Justice and Police, Department of Legislation	SITALDIN	Randhir
Trinidad and Tobago	Ministry of Public Administration, Legal Services Division	MAHARAJ	Vashti
Trinidad and Tobago	Telecommunications Authority of Trinidad and Tobago	PHILIP	Corinne
Trinidad and Tobago	Ministry of Public Administration, ICT Secretariat	SWIFT	Kevon

Regional/International Organizations' Participants

Organization	Last Name	First Name
Caribbean Community Secretariat (CARICOM)	JOSEPH	Simone
Caribbean ICT Virtual Community (CIVIC)	GEORGE	Gerry
Caribbean ICT Virtual Community (CIVIC)	WILLIAMS	Deirdre
Caribbean Telecommunications Union (CTU)	WILSON	Selby
Delegation of the European Commission to Barbados and the Eastern Caribbean (EC)	HJALMEFJORD	Bo
Eastern Caribbean Telecommunications Authority (ECTEL)	CHARLES	Embert
Eastern Caribbean Telecommunications Authority (ECTEL)	GILCHRIST	John
Eastern Caribbean Telecommunications Authority (ECTEL)	HECTOR	Cheryl
International Telecommunication Union (ITU)	CROSS	Philip
International Telecommunication Union (ITU)	LUDWIG	Kerstin
Office of Trade Negotiations (formerly CRNM) Caribbean Community Secretariat (CARICOM)	BROWNE	Derek E.
Organization of Eastern Caribbean States Secretariat (OECS)	FRANCIS	Karlene

HIPCAR Consultants Participating in the Workshop

Last Name	First Name
MARTÍNS DE ALMEIDA	Gilberto
GERCKE	Marco
MORGAN[45]	J Paul
PRESCOD	Kwesi

45 Workshop Chairperson

Annex 2

Participants of the Second Consultation Workshop (Stage B) for HIPCAR Project Working Group dealing with ICT Legislative Framework – Information Society Issues
Frigate Bay, Saint Kitts and Nevis, 19 – 22 July 2010

Officially Designated Participants and Observers

Country	Organization	Last Name	First Name
Antigua and Barbuda	Ministry of Information, Broadcasting, Telecommunications, Science & Technology	SAMUEL	Clement
Bahamas	Utilities Regulation and Competition Authority	DORSETT	Donavon
Barbados	Ministry of Finance, Investment, Telecommunications and Energy	BOURNE	Reginald
Barbados	Office of Trade Negotiations	BROWNE	Derek
Barbados	Ministry of Trade, Industry and Commerce	NICHOLLS	Anthony
Belize	Ministry of Finance	LONGSWORTH	Michelle
Belize	Public Utilities Commission	PEYREFITTE	Michael
Dominica	Ministry of Information, Telecommunications and Constituency Empowerment	CADETTE	Sylvester
Dominica	Ministry of Legal Affairs	RICHARDS-XAVIER	Pearl
Grenada	National Telecommunications Regulatory Commission	FERGUSON	Ruggles
Grenada	National Telecommunications Regulatory Commission	ROBERTS	Vincent
Guyana	Public Utilities Commission	PERSAUD	Vidiahar
Guyana	Office of the President	RAMOTAR	Alexei
Guyana	National Frequency Management Unit	SINGH	Valmikki
Jamaica	Office of the Prime Minister	MURRAY	Wahkeen
Jamaica	Attorney General's Chambers	SOLTAU-ROBINSON	Stacey-Ann
Jamaica	Digicel Group	GORTON	Andrew
Jamaica	LIME	SUTHERLAND CAMPBELL	Melesia
Saint Kitts and Nevis	Ministry of National Security	ARCHIBALD	Keisha
Saint Kitts and Nevis	Department of Technology	BOWRIN	Pierre
Saint Kitts and Nevis	ICT4EDC Project	BROWNE	Nima
Saint Kitts and Nevis	Government of St. Kitts and Nevis	CHIVERTON	Eurta
Saint Kitts and Nevis	Department of Technology	HERBERT	Christopher
Saint Kitts and Nevis	Ministry of Youth Empowerment, Sports, Information Technology, Telecommunications and Post	LAZAAR	Lloyd
Saint Kitts and Nevis	Ministry of Finance, Financial Intelligence Unit	MASON	Tracey
Saint Kitts and Nevis	Ministry of Sustainable Development	MUSSENDEN	Amicia
Saint Kitts and Nevis	Ministry of Youth Empowerment, Sports, Information Technology, Telecommunications and Post	PHILLIP	Glen

Annex 2

Country	Organization	Last Name	First Name
Saint Kitts and Nevis	Attorney General's Chambers	POWELL WILLIAMS	Tashna
Saint Kitts and Nevis	Ministry of Finance, Financial Intelligence Unit	SOMERSALL-BERRY	Jacqueline
Saint Kitts and Nevis	Ministry of Youth Empowerment, Sports, Information Technology, Telecommunications and Post	WHARTON	Wesley
Saint Lucia	Ministry of Communication, Works, Transport and Public Utilities	DANIEL	Ivor
Saint Lucia	Ministry of Communications, Works, Transport and Public Utilities	FELICIEN	Barrymore
Saint Lucia	Cable & Wireless (St. Lucia) Ltd.	LEEVY	Tara
Saint Lucia	The Attorney General's Chambers	VIDAL-JULES	Gillian
Saint Vincent and the Grenadines	Ministry of Telecommunications, Science, Technology and Industry	ALEXANDER	K. Andre
Saint Vincent and the Grenadines	Ministry of Telecommunications, Science, Technology and Industry	FRASER	Suenel
Suriname	Telecommunicatiebedrijf Suriname (TELESUR)	JEFFREY	Joan
Suriname	Telecommunicatie Autoriteit Suriname	LETER	Meredith
Suriname	Ministry of Justice and Police	SITLADIN	Vyaiendra
Suriname	Ministry of Transport, Communication and Tourism	SMITH	Lygia
Trinidad and Tobago	Office of the Prime Minister, Information Division	MAHARAJ	Rishi
Trinidad and Tobago	Ministry of Public Administration, Legal Services Division	MAHARAJ	Vashti
Trinidad and Tobago	Telecommunications Authority of Trinidad and Tobago	PHILIP	Corinne
Trinidad and Tobago	Ministry of Public Administration, ICT Secretariat	SWIFT	Kevon

Regional/International Organizations' Participants

Organization	Last Name	First Name
Caribbean Community Secretariat (CARICOM)	JOSEPH	Simone
Caribbean ICT Virtual Community (CIVIC)	HOPE	Hallam
Caribbean ICT Virtual Community (CIVIC)	ONU	Telojo
Eastern Caribbean Telecommunications Authority (ECTEL)	WRIGHT	Ro Ann
International Telecommunication Union (ITU)	CROSS	Philip
International Telecommunication Union (ITU)	LUDWIG	Kerstin
Organization of Eastern Caribbean States Secretariat (OECS)	FRANCIS	Karlene

Annex 2

HIPCAR Consultants Participating in the Workshop

Last Name	First Name
GERCKE	Marco
MORGAN[46]	J Paul
PRESCOD	Kwesi

46 Workshop Chairperson.

International Telecommunication Union
Telecommunication Development Bureau (BDT)
Place des Nations
CH-1211 Geneva

E-mail: bdtmail@itu.int
www.itu.int/ITU-D/projects/ITU_EC_ACP/

Geneva, 2013