

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

Access to Public Information (Freedom of Information): Model Policy Guidelines & Legislative Texts

HIPCAR

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



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

Access to Public Information (Freedom of Information):

Model Policy Guidelines
& Legislative Texts

HIPCAR

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



Disclaimer

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

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



Please consider the environment before printing this report.

© ITU 2013

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

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 through three separate sub-projects customized to the specific needs of each region: the Caribbean (HIPCAR), sub-Saharan Africa (HIPSSA) and the Pacific Island Countries (ICB4PAC).

The HIPCAR Steering Committee – chaired by the Caribbean Telecommunications Union (CTU) – provided guidance and support to a team of consultants, including Mr. Gilberto Martins de Almeida, Ms. Pricilla Banner 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 organizations, 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 a document such as this, reflecting the overall requirements and conditions of the Caribbean region while also representing international best practice.

The activities have been implemented by Ms Kerstin Ludwig, responsible for the coordination of activities in the Caribbean (HIPCAR Project Coordinator), and Mr Sandro Bazzanella, responsible for the management of the whole project covering sub-Saharan Africa, the Caribbean and the Pacific (ITU-EC-ACP Project Manager) with the overall support of Ms Nicole 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

	<i>Page</i>
Foreword	iii
Acknowledgements	v
Table of Contents	vii
Introduction	1
Section I: Model Policy Guidelines – Access to Public Information (Freedom of Information)	9
Section II: Model Legislative Text – Licensing Access to Public Information (Freedom of Information)	13
Arrangement of Sections.....	13
PART I – PRELIMINARY	15
PART II – DUTY TO PUBLISH CERTAIN INFORMATION.....	17
PART III – THE RIGHT OF ACCESS TO PUBLIC INFORMATION.....	19
PART IV – EXEMPT DOCUMENTS.....	23
PART V – REVIEW AND APPEALS	26
PART VI – DESIGNATED AUTHORITY	27
PART VII – CONTRAVENTION AND ENFORCEMENT	31
PART VIII – MISCELLANEOUS.....	33
Section III: Explanatory Notes to Model Legislative Text on Access to Public Information (Freedom of Information)	35
INTRODUCTION	35
COMMENTARY ON SECTIONS	36
PART I – PRELIMINARY CLAUSES	36
PART II – GENERAL DUTY OF PUBLIC BODIES TO PUBLISH INFORMATION.....	39
PART III – GENERAL RIGHT OF INDIVIDUALS TO ACCESS PUBLIC INFORMATION	40
PART IV – EXEMPTION OF DOCUMENTS OR INFORMATION WITHIN DOCUMENTS.....	43
PART V – REVIEW OF AND APPEAL OF THE DECISIONS OF PUBLIC AUTHORITIES	44
PART VI – ESTABLISHING THE DESIGNATED AUTHORITY, ITS APPROPRIATE FORM AND POWERS.....	45
PART VII – ESTABLISHING OFFENCES AND PENALTIES FOR BREACH OF PROVISIONS	49
PART VIII – GENERAL PROVISIONS TO FACILITATE IMPLEMENTATION OF THE FRAMEWORK	50
ANNEXES	53
Annex 1 Participants of the First Consultation Workshop for HIPCAR Project	53
Annex 2 Participants of the Second Consultation Workshop (Stage B) for HIPCAR Project	55

Introduction

1.1. HIPCAR Project – Aims and Beneficiaries

The HIPCAR project¹ was officially launched in the Caribbean by the International Telecommunication Union (ITU) and the European Commission (EC) 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 sub-Saharan Africa and the Pacific.

HIPCAR's objective is to assist CARIFORUM² 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 Organizations (CANTO), Caribbean ICT Virtual Community (CIVIC), and International Telecommunication Union (ITU).

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 set at EUR 8 million and a complement of USD 500,000 by the International Telecommunication Union (ITU). It is implemented by 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 organization 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.

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 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 Access to Public Information (Freedom of Information), 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 report³ – involved a comparative analysis of current legislation on Access to Public Information 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 “Access to Public Information: Assessment Report” available at www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/

The model legislative text on Access to Public Information 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. Pricilla Banner, and the second stage by Mr. Gilberto Martins de Almeida. Following this, the draft model policy guidelines were prepared by Mr. Martins de Almeida, and then reviewed, discussed and finalized by the HIPCAR Working Group on Information Society Issues during the project's First Consultation Workshop for the above Working Group held in Saint Lucia on 8-12 March 2010. Based on the model policy guidelines, the HIPCAR consultant Mr. Kwesi Prescod prepared the draft model legislative text, which was also reviewed, discussed and finalized by the above Working Group during the project's Second Consultation Workshop held in Saint Kitts and Nevis on 19 - 22 July 2010 (see Annexes). The explanatory notes to the model legislative text were prepared by Mr. Prescod addressing, *inter alia*, the points raised at the second workshop. The documents were endorsed by a broad consensus at these workshops. The HIPCAR Project Steering Committee and the Project Management Team oversaw the process of developing these documents.

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 Access to Public Information (Freedom of Information)

In the so-called Information Society, in which information is a common currency and therefore expected to flow globally, every State is admitted to participate and contribute in the international sharing of information. As a result, States where domestic policies and legislation do not expressly enable such sharing tend not to be seen as open and welcoming environments for exchange of information, and remain aside from important flows of information such as those associated with financial investments, health, private data, and many others. In other words, a State where information sharing is not clearly encouraged is expected to enjoy a lower chance for achieving favourable insertion in the global arena.

Information sharing presupposes freedom of information. As a matter of fact, without free access to information, there is little, or no, information to be shared. Freedom, in this context, means legal mandates and duties imposed so as to ensure that information is compulsorily disclosed once requested in accordance with specific statutory law provisions.

Similarly, freedom of information is a corollary of freedom of expression and of privacy rights. The integrated enforcement of such principles has been an international concern, acknowledged in several international forums including the World Summit on the Information Society (WSIS) – where the Declaration of Principles⁴ adopted in 2003 made the following specific reference to freedom of information:

"We reaffirm, as an essential foundation of the Information Society, and as outlined in Article 19 of the Universal Declaration of Human Rights, that everyone has the right to freedom of opinion and of expression; that this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers. Communication is a fundamental social process, a basic human need and the foundation of all social organisation. It is central to the Information Society. Everyone, everywhere should have the opportunity to participate and no one should be excluded from the benefits the Information Society offers."

⁴ International Telecommunication Union (2003). World Summit on the Information Society. "Declaration of Principles." www.itu.int/wsis/docs/geneva/official/dop.html

Such international consensus has translated into a large number of States which have either implemented legislation on freedom of information or have considered its adoption.⁵

Wide-spread national laws on freedom of information are due not only to international considerations, but also to the fact that they favour democracy and political stability – which are pre-requisites for national or regional social and economic development. Freedom of Information is deemed to create an enabling environment for democratic governance by providing openness, transparency and accountability within government.

A Freedom of Information Act (“FOIA”) allows citizens to have direct and enforceable right of access to information held by public bodies or by private bodies exercising public functions (governmental and quasi governmental entities), as well as to information held by private parties where access to which has not been restrained. Such direct access allows citizens to have more frank and informed interactions with the government and to participate in democratic governance in more meaningful ways. This includes the citizen’s ability to participate in the formation of discourses aimed at influencing government’s decision-making, as well as to critically scrutinize government policies and actions for the purpose of improving policies and actions and keeping government accountable.

Empowerment of citizens with information concerning official policy-making contributes to the flourishing of participatory democracy. Therefore, relevant legislation allows citizens to effectively monitor government’s activities in pursuit of good governance and to ensure that the government is honouring its duties vis-à-vis its country’s citizenry. On the other hand, it also allows governments to build an environment of trust and confidence with its citizens. By the same token, FOIA recognizes the detrimental effect which the disclosure of certain information may have on the public or community interests or on private or business interests of persons where the government is the keeper of such information by law. FOIA, thus, seeks to balance these competing interests by providing for disclosure of or access to information generally, with specified exceptions which vary from one jurisdiction to another.

This need for balance is particularly pertinent in view of the manner in which information and communication technology has changed the landscape of information storage, maintenance, dissemination, management and the like. Digital social inclusion and citizenship, concerns with cyber security, and electronic government are some examples, among others, of domains which shall be considered for building such a balance.

Freedom of Information laws generally contain certain fundamental principles which are necessary for the law to achieve its purpose. In this regard, FOIA normally includes a presumption in favour of disclosure of information, procedural guidelines which provide the manner in which the right of access is exercised and the information is obtained, specified exemptions to the right of access, and the right of appeal to an independent body regarding any claimed refusal or breach of the right to access information. Ideally, FOIA should also contain concrete measures to ensure proper training and effective implementation and enforcement, as well as protection of individuals who release information in good faith.

⁵ According to Mazhar Siraj (2010). ["Exclusion of Private Sector from Freedom of Information Laws: Implications from a Human Rights Perspective"](#). *Journal of Alternative Perspectives on Social Sciences* 2 (1): 213. www.japss.org/upload/11_Mazhar%5B1%5D.pdf, quoted in [www.en.wikipedia.org/wiki/Freedom_of_information#Freedom_of_information_legislation](http://en.wikipedia.org/wiki/Freedom_of_information#Freedom_of_information_legislation), “As of 2006 70 countries had comprehensive freedom of information legislation for public bodies, nearly half of which had been enacted in the past 10 years. Such legislation was pending in a further 50 countries”.

Section I: Model Policy Guidelines – Access to Public Information (Freedom of Information)

Following, are the Model Policy Guidelines that a country may wish to consider in relation to Access to Public Information (Freedom of Information).

1. CARICOM/CARIFORUM COUNTRIES SHALL AIM TO ESTABLISH NECESSARY COMMON INTERPRETATIONS FOR KEY TERMS ASSOCIATED WITH FREEDOM OF INFORMATION⁶

- There shall be proper definition of “information”, “communication”, “data”, “record”, and “document”.
- There shall be sufficiently broad wording in the definition of these terms, coupled with a list of illustrative examples.
- There shall be comprehensive scope of media, source of information, and date of production subject to interception of communication, so that it encompasses electronic or non-electronic documents, tapes, films, sound recording, images, produced by a public party or by a private party, at any time.

2. CARICOM/CARIFORUM COUNTRIES SHALL AIM TO ESTABLISH THE NECESSARY FRAMEWORK TO DEFINE THE PUBLIC OR PRIVATE ORIGIN, AND ROLE, OF THE PARTIES IN CHARGE OF MANAGING FREEDOM OF INFORMATION

- There shall be provision in law which explicitly states what is the role of “public authorities”, “prescribed authorities” and “private bodies”, and “social communication media” in the management of freedom of information.
- There shall be provision establishing that public authority in freedom of information laws should extend to any body which carries out government functions.
- There shall be provision establishing that, in certain instances, freedom of information shall extend to private entities once those entities are clearly providing an essential and/or permanent public service.
- There shall be provision for the production and enforcement of technical standards designed to foster freedom of information.
- There shall be provision recognizing co- and self-regulation in certain sectors of markets or of activities.
- There shall be definition on what characterizes “press” and is therefore protected under the laws which regulate press activity.
- There shall be public policy harmonizing freedom of information and intellectual property, with regard to information produced by government or by private parties in the exercise of public function.
- There shall be public policy encouraging institutional cooperation for development of databases and other mechanisms of storage or publication of data which are instrumental for achieving the goals of freedom of information.

⁶ There shall be public campaign to develop awareness on the right to freedom of information, and explaining the public policies which address it.

3. CARICOM/CARIFORUM COUNTRIES SHALL DEFINE THE LEGAL MANDATES AND THE STANDARDS TO WHICH FREEDOM OF INFORMATION SHALL BE BOUND

- The law/legal mandate should be enabling in nature and refrain from being overly prescriptive in its provisions.
- The law/legal mandate shall state that no official document shall be kept confidential unless there are overriding public interest reasons to the contrary.
- The law/legal mandate shall specify which are the constitutional grounds of freedom of information, in order to establish the weight it must have vis-à-vis other constitutional rights or principles.
- The law/legal mandate shall provide for automatic publication of certain types of information which shall be immediately made available to the public.
- The law/legal mandate shall provide for publication of information in electronic and in non-electronic media, in order to guarantee full accessibility.
- The law/legal mandate shall provide for appropriate standards of update, storage, and discard of information.
- The law/legal mandate shall determine that the management of freedom of information be guided by the objectives of security, efficiency, effectiveness and user-friendly records management.
- The law/legal mandate shall define guidelines to be followed in the selection of search or filter mechanisms associated with availability of information of public interest.

4. CARICOM/CARIFORUM COUNTRIES SHALL DEFINE EXEMPTIONS FROM COMPLIANCE WITH FREEDOM OF INFORMATION⁷

- The law/legal mandate should provide for exemptions clearly and narrowly drawn, in order to avoid wide-ranging exemptions, which could defeat the purposes of freedom of information.
- The law/legal mandate shall establish that in determining whether a document is exempt from disclosure, a “public interest test” be administered.
- The law/legal mandate shall determine that documents are tested on an individual basis and are not automatically placed into an exemption class.
- The law/legal mandate shall state that where the public interest in disclosing the information is greater than the potential harm to be caused, the information should be disclosed.
- The law/legal mandate shall give special focus to the application of the public interest test, with emphasis on spreading information on relevant detailed criteria and existing interpretation, where applicable.

⁷ There should be associated development of awareness on criteria which harmonize freedom of information and various kinds of secrecy acts (banking, tax, mail, professional, judicial, and others).

5. CARICOM/CARIFORUM COUNTRIES SHALL ESTABLISH PROCEDURES FOR ENFORCEMENT, REVIEW AND APPEAL REGARDING FREEDOM OF INFORMATION

- The law/legal mandate shall establish procedures for enforcement, review and appeal in connection with freedom of information.
- The law/legal mandate shall provide for an internal review of the original decision by a designated higher authority within the public authority.
- The law/legal mandate shall provide for an independent oversight and arbitration body with the power to undertake investigations on its own accord or in response to complaints, to make binding determinations, to compel parties to take action, enforce orders and impose sanctions.
- The law/legal mandate should provide for procedures guiding the operation of the oversight body including time limits for decisions, form of notices of appeal, of decision and delegation of power.
- The law/legal mandate shall set forth the individual right of appeal to the independent oversight body (either existing or specially established for the purpose) upon refusal by a public authority to disclose information.
- The law/legal mandate shall establish that both the applicant and the public authority shall have a right of appeal to the Courts against decisions of the oversight body.
- The law/legal mandate shall establish time lines so that the response to requests and the provision of information are not delayed beyond reasonable time.
- The law/legal mandate shall define cost-effective strategies of publication, such as making information available via the Internet, etc.
- The law/legal mandate shall define whether the service of provision of information shall be charged, or not, inclusively where it is transferred to private bodies in the exercise of public function.
- The law/legal mandate shall establish sanctions for the failure to comply with duties and obligations relating to freedom of information, in order to foster its compliance.

6. CARICOM/CARIFORUM COUNTRIES SHALL PROVIDE ADEQUATE PROTECTION TO WHISTLEBLOWERS AND ANONYMOUS CHANNELS OF DENOUNCEMENT

- The law/legal mandate shall establish that individuals be protected from any legal, administrative or employment-related sanctions for releasing information on wrong-doing once they acted in good faith and in the reasonable belief that the information was substantially true and disclosed evidence of wrong-doing, as the inclusion of strong whistle-blower protection is an indication of a government’s willingness to subject itself to legitimate scrutiny.
- The law/legal mandate shall also establish anonymous channels for denouncement, in order to maximize chances of capturing report on wrong-doings.

7. CARICOM/CARIFORUM COUNTRIES SHALL ESTABLISH THE FRAMEWORK OF FREEDOM OF INFORMATION IN CONJUNCTION WITH PUBLIC POLICIES ON RELATED MATTERS

- The law/legal mandates shall regulate freedom of information in a way to ensure consistency with public policy/existing legislation on national security.
- The law/legal mandates shall regulate freedom of information in a way to ensure consistency with public policy/existing legislation on cybercrime.
- The law/legal mandates shall regulate freedom of information in a way to ensure consistency with public policy/existing legislation on interception of communication.
- The law/legal mandates shall regulate freedom of information in a way to ensure consistency with public policy/existing legislation on privacy and on data protection.
- The law/legal mandates shall regulate freedom of information in a way to ensure consistency with public policy/existing legislation on censorship.
- The law/legal mandates shall regulate freedom of information in a way to ensure consistency with public policy/existing legislation on social digital inclusion.
- The law/legal mandates shall regulate freedom of information in a way to ensure consistency with public policy/existing legislation on information security.
- The law/legal mandates shall regulate freedom of information in a way to ensure consistency with public policy/existing legislation on intellectual property.
- The law/legal mandates shall regulate freedom of information in a way to ensure consistency with public policy/existing legislation on freedom of broadcasting.
- The law/legal mandates shall regulate freedom of information in a way to ensure consistency with public policy/existing legislation on *habeas data*.

Section II: Model Legislative Text – Licensing Access to Public Information (Freedom of Information)

Following, is the Model Legislative Text that a country may wish to consider when developing national legislation relating to Access to Public Information (Freedom of Information). This model text is based on the Model Policy Guidelines outlined previously.

Arrangement of Sections

PART I. PRELIMINARY	15
1. Short Title and Commencement.....	15
2. Objective.....	15
3. Definitions	15
4. Non-Applicability of the Act	17
5. Binds the State.....	17
PART II. DUTY TO PUBLISH CERTAIN INFORMATION.....	17
6. Publication of Information Concerning Functions of Public Authorities	17
7. Certain Documents to Be Available for Inspection and Purchase	18
8. Online Publication	18
PART III. THE RIGHT OF ACCESS TO PUBLIC INFORMATION.....	19
9. Right of Access.....	19
10. Access to Certain Documents	19
11. Requests for Access/Communication.....	19
12. Duty to Assist Applicant.....	20
13. Transfer of Request for Access	20
14. Time-Limit for Determining Requests	20
15. Decisions of a Public/Prescribed Authority	20
16. Notice of Decision and Access to Documents	20
17. Fees.....	21
18. Deletion of Exempt Information.....	21
19. Forms of Access	21
20. Deferral of Access	22
21. Refusal of Access	22
22. Decisions to Be Made by Authorised Persons	23
PART IV. EXEMPT DOCUMENTS	23
23. Disclosure of Exempt Documents in the Public Interest	23
24. Cabinet Documents	23
25. Information Affecting National Security, Defence and International Relations.....	23
26. Documents Affecting Enforcement or Administration of the Law.....	24
27. Documents Affecting Legal Proceedings or Subject to Legal Professional Privileges	24

28. Documents Disclosure of which would Be Contempt of Court of Contempt of Parliament	24
29. Documents Relating to Industrial and Trade Secrets, Business Affairs	24
30. Documents Affecting the National Economy	25
31. Policy Making and Operation of Public Bodies.....	25
32. Documents Containing Material Obtained in Confidence.....	25
33. Documents Affecting Personal Privacy.....	26
PART V. REVIEW AND APPEALS.....	26
34. Applicant’s Right to an Internal Review	26
35. Internal Review.....	26
36 Applicant’s Right to an Internal Review	27
PART VI. DESIGNATED AUTHORITY	27
37. Establishment of the Designated Authority	27
38. Tenure of Office.....	28
39. Protection of the Designated Authority	28
40. Delegation of Powers by Designated Authority	28
41. Functions of the Designated Authority	28
42. Confidentiality and Oath	29
43. Powers of Designated Authority.....	29
44. Power of Designated Authority to Obtain Information.....	29
45. Contents of Information Notice	29
46. Failure or Refusal to Comply with Information Notice.....	29
47. Complaints to Designated Authority and Powers of Investigation	30
48. Form of Complaint.....	30
49. Notice of Investigation	30
50. Powers of Entry and Search and Seizure	30
51. Matters Exempt from Search, Inspection and Seizure	30
52. Investigations in Private	30
53. Power of Designated Authority to Issue Enforcement Notice	31
54. Enforcement Notice.....	31
55. Failure to Comply with Enforcement Notice an Offence.....	31
PART VII. CONTRAVENTION AND ENFORCEMENT	31
56. Breach of Record Management Rules	31
57. Obstruction of the Designated Authority.....	32
58. False Information to the Designated Authority.....	32
59. Breach of Confidentiality Oath	32
60. Breach of Whistleblower Protection	32
PART VIII. MISCELLANEOUS	33
61. Management of Official Documents	33
62. Codes of Practice	33
63. Correction of Personal Information.....	33
64. Role of the Courts.....	33
65. Report to the Parliament.....	33
66. Regulations	34

PART I – PRELIMINARY

Short Title and Commencement

1. This Act may be cited as the Freedom of Information Act, and shall come into force and effect [on xxx/ following publication in the *Gazette*].

Objective

2. (1) The objective of this Act is to extend the right of members of the public to access to information in the possession of public [*or of prescribed*] authorities [in accordance with the principles that such information should be available to the public] by -

- a. making available to the public information about the operations of public authorities and, in particular, ensuring that the rules and practices affecting members of the public in their dealings with public authorities are readily available to persons affected by those rules and practices;
- b. creating a general right of access to information in documentary form in the possession of public authorities limited only by specific exceptions and exemptions necessary for the protection of essential public interests and the private and business affairs of persons in respect of whom information is collected and held by public authorities;
- c. to provide a right of access to information held by private bodies where this is necessary for the exercise or protection of any right or once those entities are clearly providing an essential and/or permanent public service, subject only to limited and specific exceptions;
- d. to provide a framework where the decisions on the disclosure of such information should be reviewed independently of government;
- e. authorising and encouraging the proactive public release of appropriate government information by public authorities [subject to limitations outlined in law].

(2) The provisions of this Act shall be interpreted so as to further the object set out in subsection (1), guided by the principles of security, efficiency, effectiveness and [user-friendly] record management, and so as to facilitate and promote the prompt disclosure of information at the lowest reasonable cost.

Definitions

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

- a. “applicant” means a person who has made a request in accordance with section 14.
- b. “Designated Authority” refers to the body established in Part VII.
- c. “document” means any [medium] in which information is recorded including any correspondence, memorandum, book, plan, map, drawing, pictorial or graphic work, photograph, film, microfilm, audio, video machine-readable record and any other documentary material, regardless of physical form or characteristics, and includes electronic and non-electronic documents and any copy of those things.

- d. “official document” means a document held by a public/ prescribed authority in connection with its functions as such, whether or not it was created-
 - i. by that authority; or
 - ii. before the commencement of this Act,
 and, for the purposes of this Act, a document is held by a public authority if it is in its possession, custody or control.
- e. “Minister” means the Minister who has been assigned responsibility for [information/public administration].
- f. “personal information” means information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing –
 - i. information relating to the race, national or ethnic origin, religion, age or marital status of the individual;
 - ii. information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
 - iii. any identifying number, symbol or other particular assigned to the individual;
 - iv. the address, fingerprints or blood type of the individual;
 - v. the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual.
- g. “public authorities” includes -
 - 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, or the private office of a Minister, wherever located;
 - 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. [A body corporate which is undertaking essential public services or functions on behalf of public authorities];
 - viii. any other body designated by the Minister by regulation made under this Act, to be a public authority for the purposes of this Act;

(1A where jurisdictions do not wish to include the definition of private bodies within the definition of “public authority”, the following alternatives may be included:

Section II

Non-Applicability of the Act

- h. ["prescribed authorities" includes public authorities and private bodies
 - i. private bodies: means those enterprises that are undertaking essential public services or functions on behalf of public authorities. and that are prescribed by the Minister by Order].
4. (1) This Act does not apply to –
- a. the [President/ Governor General]; or
 - b. a commission of inquiry issued by the [President];
- (2) For the purposes of this Act -
- a. a court, or the holder of a judicial office or other office pertaining to a court in his capacity as the holder of that office, shall not be regarded as a public authority;
 - b. a registry or other office of court administration, and the staff of such a registry or other office of court administration in their capacity as members of that staff in relation to those matters which relate to court administration, shall be regarded as part of a public authority.

Binds the State

5. This Act shall bind the State.

PART II – DUTY TO PUBLISH CERTAIN INFORMATION

Publication of Information Concerning Functions of Public Authorities

6. (1) A public authority shall, with the *[approval of/in consultation with the Minister]*, cause to be published annually in the Gazette, as well as on its website or at least one -newspaper circulated nationally or in a mode approved by the Minister -
- a. a statement setting out the particulars of the organisation and functions of the public authority, indicating as far as practicable the decision-making powers and other powers affecting members of the public that are involved in those functions;
 - b. a statement of the categories of documents that are maintained in the possession of the public authority;
 - c. a statement of the material that has been prepared by the public authority under this Part for publication or inspection by members of the public, and the places at which a person may inspect or obtain that material; and
 - d. a statement of the procedure to be followed by a person when a request for access to a document is made to a public authority.

(1A – For jurisdictions where there is the inclusion of particular private bodies into the definition of “public bodies”, the legislation may facilitate the limitation of the applicability (1) above to private bodies).

Section II

Certain Documents to Be Available for Inspection and Purchase

(2) Nothing in this section requires the publication of information that is of such a nature that its inclusion in a document would cause that document to be an exempt document.

7. (1) This section applies to documents that are provided by the public/ prescribed authority for its use or the use of its officers in making decisions or recommendations in accordance with any enactment or scheme administered by the authority with respect to rights, privileges or benefits, or to obligations, penalties or other detriments, to or for which persons may be entitled or subject, including –
- a. manuals or other documents containing interpretations, rules, guidelines, practices or precedents in the nature of letters of advice providing information to bodies or persons outside the public/ prescribed authority;
 - b. documents containing particulars of such a scheme, not being particulars contained in any other enactment; and
 - c. documents containing statements of the manner, or intended manner, of administration or enforcement of such an enactment or scheme, but not including documents that are available to the public as published otherwise than by the public/ prescribed authority or as published by another public authority.

(2) A public/ prescribed authority shall -

- a. cause copies of all documents to which this section applies that are in use from time to time to be made available for inspection and for purchase by members of the public; and
- b. not later than twelve months after the date of commencement of this Act and annually thereafter, cause to be published in the Gazette, a statement (which may take the form of an index) specifying the documents of which copies are, at the time of preparation of the statement, so available and the place or places where copies may be inspected and may be purchased.

(3) This section does not require a document of the kind referred to in subsection (1) containing sensitive information that would make the document an exempt document to be made available in accordance with subsection (2), but, if such a document is not so made available, the public authority shall, if practicable, cause to be prepared a corresponding document, altered only to the extent necessary to exclude such sensitive information, and cause the document so prepared to be dealt with in accordance with subsection (2).

Online Publication

8. Every prescribed authority shall endeavor within reasonable time and subject to availability of resources that official documents covered by the provisions of Section 7 (1) are computerized and made available through such systems as to facilitate the authorized access to such documents through electronic dissemination channels which may include, but not be limited to, their official website.

PART III – THE RIGHT OF ACCESS TO PUBLIC INFORMATION

Right of Access

9. (1) Subject to this Act, every person shall have the right to access official documents or information within such documents held by public/ prescribed authorities.
- (2) Subject to Part IV of this Act, no official document or information within such document shall be kept confidential unless there are overriding public interest reasons to the contrary.
- [(3) The exemption of an official document or part thereof from disclosure shall not apply after the document has been in existence for twenty years or such shorter or longer period as the Minister may specify by order subject to affirmative resolution.]
- (4) Nothing in this Act shall prevent a public/ prescribed authority from publishing or giving access to documents (including exempt documents), otherwise than as required by this Act, where it has the discretion to do so or is required by law to do so.

Access to Certain Documents

10. (1) Any applicant requesting information in a document from a public authority shall be entitled, subject only to the provisions of Parts III and IV of this Act: –
- a. to be informed whether or not the public authority holds a document containing that information or from which that information may be derived; and
 - b. if the public authority does hold such a document, to have that information provided to him.

(1A – For jurisdictions which have merged particular private bodies into the definition of “public authority” there may be an opportunity to explicitly exclude such private parties from (1) above, or treat with this group of persons differently to the treatment of public sector bodies.)

(2) Where –

- a. a document is open to public access, as part of a public register or otherwise, in accordance with another enactment; or
- b. a document is available for purchase by the public in accordance with arrangements made by a prescribed authority,

the access to that document shall be obtained in accordance with that enactment or arrangement, as the case may be.

Requests for Access/Communication

11. (1) Subject to subsection (3), a person who wishes to obtain access to an official document of a prescribed authority shall make a request in writing to the relevant public/ prescribed authority for such access.
- (2) A request shall identify the document or shall provide such information concerning the document as is reasonably necessary to enable the public/ prescribed authority to identify the document.
- (3) A public/ prescribed authority may prescribe a form for requests for information, provided that such forms do not unreasonably delay requests or place an undue burden upon those making requests.

Section II

- Duty to Assist Applicant** 12. (1) A public/ prescribed authority shall take reasonable steps to assist any person who -
- a. wishes to make a request under section 14; or
 - b. has made a request which does not comply with the requirements of section 14(2), to amend such request so that it is in a manner which complies with that subsection,
 - c. due to illiteracy or disability, is unable to make a written request for information pursuant to section 14(1).
- Transfer of Request for Access** 13. (1) Where a request is made to a public/ prescribed authority for access to an official document and the request has not been directed to the appropriate public/ prescribed authority, the authority to which the request is made shall transfer the request to the appropriate public/ prescribed authority and notify the person making the request accordingly.
- (2) Where a request is transferred to a public/ prescribed authority in accordance with this section, it shall be deemed to be a request made to that public authority and received on the date of transfer.
- Time-Limit for Determining Requests** 14. (1) A public/ prescribed authority shall take reasonable steps to notify an applicant of the decision on a request as soon as practicable but in any case not later than [thirty working days] from the date on which the request is made.
- (2) Where a request for information relates to information which reasonably appears to be necessary to safeguard the life or liberty of a person, a public/ prescribed authority may be obliged to render a response within [two days].
- [(3) Notwithstanding subsection (1), a public/ prescribed authority may, by notice in writing within the initial period under subsection (1), extend the period in sub-section (1) to the extent strictly necessary, and in any case to not more than [forty working days], where the request is for a large number of records or requires a search through a large number of records, and where compliance within initially public/ prescribed period would unreasonably interfere with the activities of the authority.]
- (4) Failure to comply with this section is deemed to be a refusal of the request.
- Decisions of a Public/Prescribed Authority** 15. A decision of a public/ prescribed authority in relation to a request may provide for:
- a. Provision of access to all or part of the relevant documents;
 - b. The deferral of provision of access to all or part of relevant documents; or
 - c. The refusal of access to the relevant document with reasons for such refusal.
- Notice of Decision and Access to Documents** 16. (1) Notification of the decision on a request shall be by notice in writing and state: –
- a. the applicable fee, if any, pursuant to section 19, in relation to any part of the request which is granted, and the forms of access under section 21.
 - b. adequate reasons for the refusal in relation to any part of the request which is not granted, subject only to Part IV of this Act;

Section II

- c. in relation to any refusal to indicate whether or not the public/ prescribed authority holds a record containing the relevant information, the fact of such refusal and adequate reasons for it; and
- d. any right of appeal the person who made the request may have.
- (2) Where a request for access to a document is duly made, and –
- a. the request is approved by the public/ prescribed authority; and
- b. the applicable fee required to be paid before access is granted has been paid,
- access shall be given in accordance with this Act.
- Fees** 17. (1) The Minister may, pursuant to the recommendation of the Designated Authority, by regulation –
- a. prescribe the fee payable where access to a document is to be given in the form of printed or electronic copies or copies in some other form such, as on tape, disk, film or other material;
- b. prescribe the manner in which any fee payable under Section 18 is to be calculated and the maximum amount it shall not exceed; and
- c. exempt any person or category of persons from paying any fees under this Act, where the information contained in the document for which access is requested is in the public interest.
- d. exclude any document or category of document from requiring a fee for access, pursuant to the provisions of Section 7 (2).
- (2) The prescribed fee shall not exceed the actual cost of searching for, preparing and communicating the document or information.
- Deletion of Exempt Information** 18. (1) Where –
- a. a decision may be made not to grant a request for access to a document on the ground that it is an exempt document;
- b. it is practicable for the public/ prescribed authority to grant access to a copy of the document with such deletions as to make the copy not an exempt document; and
- c. it appears from the request, or the applicant subsequently indicates, that the applicant would wish to have access to such a copy,
- the public/ prescribed authority shall give the applicant access to such a copy of the document.
- (2) Where access is granted to a copy of a document in accordance with subsection (1), the applicant shall be informed that it is such a copy and also be [notified] of the provisions of this Act by virtue of which any information deleted is exempt information.
- Forms of Access** 19. (1) Access to a document may be given to a person in one or more of the following forms:
- a. a reasonable opportunity to inspect the document;
- b. provision by the public/prescribed authority of a copy of the document;
- c. in the case of a document that is an article or thing from which sounds or visual images are capable of being reproduced, the making of arrangements for the person to hear or view those sounds or visual images; or

d. in the case of a document by which words are recorded in a manner in which they are capable of being reproduced in the form of sound or in which words are contained in the form of shorthand writing or in codified form, provision by the public/ prescribed authority of a written transcript of the words recorded or contained in the document

(2) Subject to subsection (3) and to section 20, where the applicant has requested access in a particular form, access shall be given in that form.

(3) If the form of access requested by the applicant -

- a. would interfere unreasonably with the operations of the public/ prescribed authority; or
- b. would be detrimental to the preservation of the document or, having regard to the physical nature of the document, would not be appropriate; or
- c. would involve an infringement of copyright (other than copyright owned by the Government) subsisting in the document access in that form may be refused and access given in another form.

(4) Where an official document exists in more than one language, communication of the document shall, from among those languages, be given in accordance with the language preference of the person making the request.

Deferral of Access

20. (1) A public/ prescribed authority which receives a request may defer the provision of access to the document concerned until the incident of a particular event (including the taking of some action required by law or some administrative action), or until the expiration of a specified time, where it is reasonable to do so in the public interest or having regard to normal and proper administrative practices.

(2) Where the provision of access to a document is deferred in accordance with subsection (1), the public/ prescribed authority shall, in informing the applicant of the reasons for the decision, indicate, as far as practicable, the period for which the deferment will be valid.

(3) the Designated Authority may from time to time review the documents and circumstances in which subsection (1) applies and establish maximum periods of deferral beyond which public/ prescribed authorities shall require particular authorisation of the Designated Authority.

Refusal of Access

21. A public/ prescribed authority dealing with a request may refuse to grant access to a document if –

- a. the public/ prescribed authority is satisfied that the work involved in processing the request would substantially and unreasonably interfere with the normal operations of the public/ prescribed authority, [and, where the public/ prescribed authority has taken reasonable steps to assist the applicant to reformulate the application so as to avoid causing such interference];
- b. the public/ prescribed authority is satisfied that the document or information within the document to be exempt from disclosure in accordance with Part IV of this Act; or
- c. the public/ prescribed authority is satisfied that the request for information is vexatious

Decisions to Be Made by Authorised Persons

22. A decision in respect of a request made to a [public/ prescribed] authority shall be made [by the responsible Minister], or the Head of the public authority or, by an officer of the prescribed authority acting within the scope of authority exercisable by him in accordance with the arrangements approved by the Minister or Head of the [public/prescribed] authority.

PART IV – EXEMPT DOCUMENTS

Disclosure of Exempt Documents in the Public Interest

23. (1) Notwithstanding any law to the contrary, a public/ prescribed authority shall give access to a document which would otherwise be deemed to be exempt where there is reasonable evidence that significant -
- a. abuse of authority or neglect in the performance of official duty;
 - b. injustice to an individual;
 - c. danger to the health or safety of an individual or of the public; or
 - d. unauthorised use of public funds,
- has or is likely to have occurred or in the circumstances giving access to the document is justified in the public interest having regard both to any benefit and to any damage that may arise from doing so.
- (2) Pursuant to subsection (1), a public/ prescribed authority shall administer appropriate tests on official documents on an individual basis to ascertain whether conditions (a) through (d) apply before determining whether a document is exempt.

Cabinet Documents

24. (1) A document is an exempt document if it is –
- a. a document that has been submitted to the Cabinet for its consideration or is proposed by a Minister of Government to be so submitted;
 - b. an official record of any deliberation or decision of the Cabinet;
 - c. a document that is a draft of copy of, or of a part of, or contains an extract from, a document referred to in paragraph (a) or (b); or
 - d. a document the disclosure of which would involve the disclosure of any deliberation or decision of the Cabinet, other than a document by which a decision of the Cabinet was officially published.
- (2) Subsection (1) does not apply to a document that contains purely statistical, technical or scientific material unless the disclosure of the document would involve the disclosure of any deliberation or decision of Cabinet.
- (3) In this section, any reference to “Cabinet” shall be read as including a reference to a committee of the Cabinet.

Information Affecting National Security, Defence and

25. (1) Information is deemed exempt if disclosure of the information or relevant documents under this Act would be contrary to the public interest for the reason that the disclosure –
- a. would prejudice the security, defence or international relations of [name of country];

Section II

International Relations		<ul style="list-style-type: none"> b. would divulge any information or matter communicated in confidence by or on behalf of the Government of another country to the Government of [name of country].
Documents Affecting Enforcement or Administration of the Law	26.	<p>A document is an exempt document if its disclosure under this Act would, or would be reasonably likely to –</p> <ul style="list-style-type: none"> a. prejudice the investigation of a breach or possible breach of the law or the enforcement or proper administration of the law in a particular instance; b. prejudice the fair trial of a person or the impartial adjudication of a particular case; c. disclose, or enable a person to ascertain the identity of a confidential source of information in relation to the enforcement or administration of the law; d. disclose methods or procedures for preventing, detecting, investigating, or dealing with matters arising out of breaches or evasions of the law, the disclosure of which would, or would be reasonably likely to, prejudice the effectiveness of those methods or procedures; or e. endanger the lives or physical safety of persons engaged in or in connection with law enforcement.
Documents Affecting Legal Proceedings or Subject to Legal Professional Privileges	27.	<p>A document is an exempt document if it is of such a nature that it would be privileged from production in legal proceedings on the ground of legal professional privilege.</p>
Documents Disclosure of which would Be Contempt of Court of Contempt of Parliament	28.	<p>A document is an exempt document if public disclosure of the document would, apart from this Act and any immunity of the State –</p> <ul style="list-style-type: none"> a. be in contempt of court; b. be contrary to an order made or given by a commission or by a tribunal or other person or body having power to take evidence on oath; or c. infringe the privileges of Parliament.
Documents Relating to Industrial and Trade Secrets, Business Affairs	29.	<p>(1) A document is an exempt document if its disclosure under this Act would disclose –</p> <ul style="list-style-type: none"> a. industrial and trade secrets or [sensitive commercial information] OR [any other information of a commercial value which value would or could reasonably be, expected to be destroyed or diminished if the information was disclosed]; b. information concerning the business or professional affairs of a person or an undertaking, the disclosure of which could – <ul style="list-style-type: none"> i. reasonably be expected to, unreasonably affect that person’s or undertaking’s lawful business and affairs; or

Section II

- ii. be contrary to public interest as the disclosure would be reasonably likely to prejudice the ability to obtain similar information in the future for the purpose of administration of either a law or of matters under the purview of a public authority.
- (2) The provisions of subsection (1) do not have effect in relation to a request by a person for access to a document only in the instances where the document concerns –
- a. the business or professional affairs of that person; or
 - b. the business, commercial or financial affairs of an undertaking of which that person, or a person on whose behalf that person made the request, is the proprietor.
- Documents Affecting the National Economy** 30. (1) A document is an exempt document if its premature disclosure under this Act would be contrary to the public interest by reason that it would be reasonably likely to have an adverse effect on the national economy.
- (2) The kinds of documents to which subsection (1) may apply include but are not restricted to, documents containing information relating to -
- a. currency or exchange rates;
 - b. interest rates;
 - c. taxes, including duties of customs or of excise;
 - d. the regulation or supervision of banking, insurance and other financial institutions;
 - e. proposals for expenditure;
 - f. foreign investment in [name of country]; or
 - g. borrowings by the Government.
- Policy Making and Operation of Public Bodies** 31. (1) A body may refuse to indicate whether or not it holds a record, or refuse to communicate information, where to do so would, or would be likely to: –
- a. cause serious prejudice to the effective formulation or development of government policy;
 - b. seriously frustrate the success of a policy, by premature disclosure of that policy;
 - c. significantly undermine the deliberative process in a public body by inhibiting the free and frank provision of advice or exchange of views; or
 - d. significantly undermine the effectiveness of a testing or auditing procedure used by a public body.
- (2) Sub-section (1) does not apply to facts, analyses of facts, technical data or statistical information.
- Documents Containing Material Obtained in Confidence** 32. (1) A document is an exempt document if its disclosure under this Act would divulge any information or matter communicated in confidence by or on behalf of a person or a government to a public authority, and –
- a. the information would be exempt information if it were generated by a public authority; or
 - b. the disclosure of the information under this Act would be contrary to the public interest by reason that the disclosure would be reasonably likely to impair the ability of a public authority to obtain similar information in the future.

**Documents
Affecting
Personal
Privacy**

- (2) This section does not apply to information –
 - a. acquired by a public authority from a business, commercial or financial undertaking; and
 - b. that relates to trade secrets or other matters of a business, commercial or financial nature.
- 33. (1) A document is an exempt document if its disclosure under this Act would involve the unreasonable disclosure of personal information of any individual.

(2) Subject to subsection (4), the provisions of subsection (1) do not have effect in relation to a request by a person for access to his own personal information [in which case such a request shall be treated as a request under the Privacy and Data Protection Act.].

(3) Where a request by a person other than a person referred to in subsection (2) is made to a public authority for access to a document containing personal information of any individual (including a deceased individual) and the public authority decides to grant access to the document, the public authority shall proceed in accordance with the Data Protection Act in deciding to grant the request and in undertaking actions upon that decision.

PART V – REVIEW AND APPEALS

**Applicant’s
Right to an
Internal
Review**

- 34. (1) Subject to subsection (4), an applicant for access to an official document may, in accordance with subsection (4), apply for an internal review of a decision by a prescribed authority to –
 - a. refuse to grant access to the document;
 - b. grant access only to some of the documents specified in an application;
 - c. defer the grant of access to the document;

(2) An applicant for amendment or annotation of a personal record may, in accordance with subsection (4), apply for a review of a decision by a prescribed authority to refuse to make that amendment or annotation.

(3) For the purposes of subsections (1) and (2), a failure to give a decision on any of the matters referred to in subsection (1) or to amend or annotate a personal record within the time required by this Act shall be regarded as a refusal to do so.

(4) An application under subsection (1) or (2) may only be made where the decision to which the application relates was taken by a person other than the responsible Minister, Head of the prescribed authority concerned.

**Internal
Review**

- 35. (1) An internal review shall be conducted –
 - a. by the responsible Minister in relation to documents referred to in sections 26, 27, 28 and 32;
 - b. in any other case, by the Head of the public/prescribed authority.

**Applicant’s
Right to an
Internal
Review**

- (2) An application for internal review shall be made —
- a. within thirty days after the date of a notification (in this subsection referred to as the initial period) to the applicant of the relevant decision, or within such further period, not exceeding thirty days, as the public authority may permit; or
 - b. where no such notification has been given, within thirty days after the expiration of the period allowed for the giving of the decision or of any other period permitted by the authority.
- (3) A person who conducts an internal review—
- a. may take any decision in relation to the application which could have been taken on an original application;
 - b. shall take that decision within a period of thirty days after the date of receipt of the application.

36. An appeal shall lie from a decision made pursuant to Section 37 (3) (a), to the Designated Authority

PART VI – DESIGNATED AUTHORITY⁸

**Establishment
of the
Designated
Authority**

37. (1) Subject to subsection (2), there shall be a Designated Authority 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 the Designated Authority if he –
- a. is a Minister, Parliamentary Secretary, or a Member of the House of Representatives; or
 - b. is a judge or magistrate; or
 - c. is public officer; or is a member of a local authority; or
 - d. is an undischarged bankrupt; or
 - e. has at any time been convicted of any offence involving dishonesty.
- (3) The Designated Authority shall appoint such staff as may be necessary to carry out his function under this Act.
- (4) The [Head of State] shall, after he has consulted the [*Prime Minister and the Leader of the Opposition,*] appoint a person who is qualified to be appointed as a temporary Designated Authority if –
- a. the Designated Authority resigns or if his office is otherwise vacant;
 - b. the Designated Authority is for any reason unable to perform the functions of his office; or

⁸ Jurisdictions have the option to structure the Designated Authority as a Commission, Council, Authority or such other body as it sees fit, and all relevant provisions would be adjusted accordingly.

Section II

		<ul style="list-style-type: none"> c. the Designated Authority 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 Designated Authority when a Designated Authority is appointed to fill the vacancy or, as the case may be, when the Designated Authority who was unable to perform the functions of his office resumes those functions or, in the case of a temporary purpose, the temporary Designated Authority has performed the function assigned to him.
Tenure of Office	38.	<p>(1) The Designated Authority shall hold office for a term not exceeding [...] years and shall be eligible for reappointment on the expiration of his term of office.</p> <p>(2) Subject to the provisions of subsection (3), the Designated Authority vacates his office-</p> <ul style="list-style-type: none"> a. at the expiration of the term for which he was appointed; b. if he becomes disqualified by virtue of subsection 39(2); or c. if he is appointed to any other office of emolument or engages in any other occupation for reward; <p>(3) The Designated Authority 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 misbehaviour.</p>
Protection of the Designated Authority	39.	No action or other proceeding for damages shall be instituted against a Designated Authority 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 Designated Authority	40.	The Designated Authority 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 particular purpose.
Functions of the Designated Authority	41.	<p>The Designated Authority shall-</p> <ul style="list-style-type: none"> a. ensure compliance with this Act and the Regulations; b. investigate reports and claims from applicants on violations of this Act or its Regulations and take remedial action as the Designated Authority deems necessary or as may be public/ prescribed under this Act, and to inform the applicants of the outcome; c. issue such directions or public statements as may be required of the Designated Authority for the purposes of this Act; d. generally monitor compliance by public/ prescribed authorities with the provisions of this Act; e. prepare and issue or approve, in consultation with the Minister, appropriate codes of practice or guidelines for the furtherance of access to public information; f. provide advice, with or without request, to a public/ prescribed authority on any matter relevant to the operation of this Act;

Section II

- g. do any thing incidental or conducive to the performance of any of the preceding functions; and
 - h. exercise and perform such other functions as are conferred or imposed on the Designated Authority by or under this Act, or any other enactment.
- Confidentiality and Oath**

42. (1) The [members of the] Designated Authority 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 [a member of] the Designated Authority, an officer of the Designated Authority’s staff or an agent of the Designated Authority shall not make use of or divulge, either directly or indirectly, any information 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.
- Powers of Designated Authority**

43. The Designated Authority shall have power, for the purpose of carrying out its functions to do all such acts as appear to it to be requisite, advantageous or convenient for, or in connection with the carrying out of these functions.
- Power of Designated Authority to Obtain Information**

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

 - a. information about and documentation of the storage of public information;
 - b. any other information in relation to matters specified in the notice as is necessary or expedient for the performance by the Designated Authority of his functions and exercise of his powers and duties under this Act.

(2) Where the information requested from a person by the Designated Authority is stored in a computer, disc, cassette, or on microfilm, or preserved by any mechanical or electronic device, the person shall produce or give access to the information in a form in which it can be taken away such that it is retrievable and accessible.
- Contents of Information Notice**

45. (1) The information notice specified in section 46 shall state-

 - a. that the person to whom the notice is addressed has a right of appeal under section [] 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**

46. (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 Designated Authority 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 [twenty five thousand dollars] or to imprisonment for a term not exceeding six months or to both.

Section II

Complaints to Designated Authority and Powers of Investigation	47.	<p>(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.</p> <p>(1) The Designated Authority may, on complaint by an applicant or at the Designated Authority'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 public/ prescribed authority in relation to an applicant.</p> <p>(2) Where a complaint is made to the Designated Authority under subsection (1), the Designated Authority shall –</p> <ul style="list-style-type: none"> a. investigate the complaint or cause it to be investigated by an authorized officer, unless the Designated Authority is of the opinion that it is frivolous or vexatious; and b. as soon as reasonably practicable, notify the applicant concerned in writing of his decision in relation to the complaint and that the applicant may, if aggrieved by the Designated Authority's decision, appeal against the decision to the Court under section 64.
Form of Complaint	48.	<p>(1) A complaint pursuant to this Act shall be made to the Designated Authority in writing unless the Designated Authority authorizes otherwise.</p>
Notice of Investigation	49.	<p>Before commencing an investigation of a complaint pursuant to this Act, the Designated Authority shall notify the Head of the public authority of the intention to carry out the investigation and shall include in the notification the substance of the complaint.</p>
Powers of Entry and Search and Seizure	50.	<p>(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.</p> <p>(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)].</p>
Matters Exempt from Search, Inspection and Seizure	51.	<p>The powers of inspection and seizure conferred by a warrant are not be exercisable in respect of public information which by virtue of Part IV is exempt from any of the provisions of this Act.</p>
Investigations in Private	52.	<p>(1) All investigations of a complaint pursuant to this Act shall be conducted in private.</p> <p>[(2) In the course of an investigation of a complaint under this Act by the Designated Authority, the person who made the complaint, head of the public/prescribed authority or other relevant party shall be given an opportunity to make representations.</p>

Section II

- | | | |
|--|-----|--|
| Power of Designated Authority to Issue Enforcement Notice | 53. | Where the Designated Authority is of the opinion that a public/ prescribed authority has contravened or is contravening a provision of this Act, the Designated Authority may, subject to section 57, serve an enforcement notice on the public/ prescribed authority, requiring the public/ prescribed authority 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 | 54. | <p>(1) An enforcement notice shall be in writing and shall-</p> <ul style="list-style-type: none"> a. specify the provision of this Act that, in the opinion of the Designated Authority, the public/ prescribed authority has contravened or is contravening and the reasons for the Designated Authority having formed that opinion; and b. specify the action which the Designated Authority requires the public/ prescribed authority to take; c. subject to subsection (2), inform the public/ prescribed authority of his right of appeal pursuant to section 65 and the time within which the appeal must be lodged. <p>(2) 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 65.</p> <p>(3) The Designated Authority may cancel an enforcement notice and, if he does so, shall notify in writing the person on whom it was served accordingly.</p> |
| Failure to Comply with Enforcement Notice an Offence | 55. | <p>(1) A person shall not, without reasonable excuse, fail or refuse to comply with a requirement specified in an enforcement notice.</p> <p>(2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine not exceeding twenty five thousand dollars or to imprisonment for a term not exceeding six months or to both such fine and imprisonment.</p> |

PART VII – CONTRAVENTION AND ENFORCEMENT

- | | | |
|--|-----|--|
| Breach of Record Management Rules | 56. | <p>(1) A person who wilfully destroys or damages a record or document required to be maintained and preserved under section 8 (2), commits an offence and is liable on summary conviction to a fine of [.....] or imprisonment for [.....] or both.</p> <p>(2) A person who knowingly destroys or damages a record or document which is required to be maintained and preserved under section 8 (2) while a request for access to the record or document is pending commits an offence</p> <p>and is liable on summary conviction to a fine of [.....] or imprisonment for [.....]or both.</p> |
|--|-----|--|

Section II

- Obstruction of the Designated Authority**
57. A person who wilfully obstructs the Designated Authority or any other person acting for or under the direction of the Designated Authority in the course of carrying out an audit or an investigation commits an offence and is liable upon –
- a. summary conviction, to a fine of not more than [...] dollars or to imprisonment for a term of [...] year or both; and
 - b. conviction on indictment, to a fine of not more than [...] dollars or to imprisonment for a term of not more than [...] years or both.
- False Information to the Designated Authority**
58. A person who wilfully makes a false statement to mislead or attempts to mislead the Designated Authority in the performance of his functions under this Act, commits an offence under this Act and is liable upon—
- a. summary conviction, to a fine of not more than [...] dollars or to imprisonment for a term of [...] year or both; and
 - b. conviction on indictment, to a fine of not more than [...] dollars or to imprisonment for a term of not more than [...] years or both.
- Breach of Confidentiality Oath**
59. A person who, without lawful excuse, breaches the oath of confidentiality, commits an offence and is liable on conviction to a fine not exceeding [...] dollars or to imprisonment for a term not exceeding [...] months or to both.
- Breach of Whistleblower Protection**
60. (1) 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 Designated Authority 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).
- (2) Notwithstanding subsection (1), the Designated Authority may establish anonymous channels of denouncement.
- (3) An employer who contravenes the provisions of subsection 1 commits an offence and is liable upon –
- a. summary conviction, to a fine of not more than [...] dollars or to imprisonment for a term of [...]; and
 - b. conviction on indictment, to a fine of not more than [...] dollars or to imprisonment for a term of not more than [...].

PART VIII – MISCELLANEOUS

Management of Official Documents	61.	<p>(1) The Minister may, in conjunction with the [National Archives] prescribe rules, standards and guidelines to be observed in the creation, storage, use, update and disposal of official documents and other public records.</p> <p>(2) Pursuant to subsection (1), a public/ prescribed authority shall ensure the maintenance and preservation of records in relation to its functions and a copy of all official documents which are created by it or which come at any time into its possession, custody or power, for such period of time as may be prescribed.</p> <p>(3) To ensure compliance with the standards and guidelines outlined, the Minister may authorise the Designated Authority to require the head of a public/prescribed authority or an officer recognized to act on behalf of that head to supply information, including specific answers to questions concerning the record creation, record keeping, record management and retention practices of that public authority.</p>
Codes of Practice	62.	<p>Notwithstanding the provisions of Part III, where this Act applies to private bodies the Designated Authority shall consult with the relevant stakeholders to promote the application of best practices in the provision of access to public information through the development of codes of practice through such means as —</p> <ol style="list-style-type: none"> a. providing guidance on the development of codes of practice; b. providing guidance on complaint resolution mechanisms; c. working with government and private sector bodies to promote awareness of codes of conduct among consumers; and d. taking any action that appears to the Designated Authority to be appropriate.
Correction of Personal Information	63.	<p>(1) Where a document contains personal information of an individual and that individual believes that the information is inaccurate, he shall proceed, and the public authority shall address the matter, in accordance with section 28 of the Privacy and Data Protection Act.</p>
Role of the Courts	64.	<p>The Court shall have jurisdiction to hear and determine -</p> <ol style="list-style-type: none"> a. applications by the Designated Authority for any Order which the Court considers appropriate to facilitate the enforcement of any provisions of this Act; b. upon application by any person, cases involving any alleged contraventions of the provisions of this Act and make such appropriate Order in relation thereto. c. upon application by any party appealing the decisions of the Designated Authority.
Report to the Parliament	65.	<p>(1) The Designated Authority shall, as soon as practicable after the thirty-first of December of each year, prepare a report on the operation of this Act during that year and cause a copy of the report to be laid before Parliament.</p>

Section II

Regulations

- (2) Each responsible Minister shall, in relation to the public authorities within his portfolio, furnish to the Designated Authority such information as is required for the preparation of any report under this section and shall comply with any prescribed requirements concerning the furnishing of that information and the keeping of records for that purpose.
66. (1) The Minister, pursuant to consultation with the Designated Authority, may 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. the fees in respect of access to documents (including the provision of copies or transcripts) in accordance with this Act;
 - b. the officers who may make decisions on behalf of a public authority; or
 - c. requirements concerning the furnishing of information and keeping of records for the purposes of section 60;
 - d. guidelines with regard to the search or filter mechanisms associated with the availability of information to the public.
- (3) All regulations made under this Act shall be laid before Parliament as soon as may be after the making thereof and shall be subject to [negative/affirmative] resolution.

Section III:

Explanatory Notes to Model Legislative Text on Access to Public Information (Freedom of Information)

INTRODUCTION

1. This Model Access to Information Legislative Text has been prepared as a 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. Access to public information, also known as Freedom of Information (“FOI”), is generally regarded as having the potential to create an enabling environment for democratic governance, by providing openness, transparency and accountability within government. Legislation on such matter, the so-called Freedom of Information Act (“FOIA”), allows citizens to have a direct and enforceable right of access to information held by public bodies and private bodies exercising public functions (governmental and quasi governmental entities), as well as to information held by private parties and to which access has not been restrained.
3. Such direct access allows citizens to have more frank and informed interactions with government and to participate in democratic governance in more meaningful ways. This includes citizen’s ability to participate in the formation of discourses aimed at influencing government’s decision-making, as well as to critically scrutinize government policies and actions, for the purpose of improving policies and actions and keeping government accountable.
4. Empowerment of citizens with information concerning official policy-making contributes to the flourishing of participatory democracy. Therefore, relevant legislation allows citizens to effectively monitor government’s activities in pursuit of good governance and ensures that government is honouring its duties vis-à-vis the citizenry. On the other hand, it also allows governments to build an environment of trust and confidence with its citizens.
5. The HIPCAR Model Legislative Text on Access to Public Information is based on the Policy Building Blocks developed within earlier phases of the HIPCAR Project⁹. These Building Blocks reviewed international best practice of the objectives, key common tools and precedents, and identified the major policy positions and systems that would need to be enshrined within legislative frameworks across the region.¹⁰ The Model Legislative Texts attempts to encode the policy guide into a legislative tool which attempts to balance the competing impetus of clarity of intent, structure and function and the necessary need of abstraction to facilitate its ready adaptation, as necessary, into the legislative framework of each HIPCAR Beneficiary State.

⁹ 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).

¹⁰ 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.

6. This Model Access to Public Information Legislative Text comprises of eight parts, and sixty-seven sections.
- **Part one** treats with preliminary considerations, such as the short title and interpretation of particular terms in the model text and treats with concerns regarding the scope of applicability of the model text.
 - **Part two** treats with establishing a general obligation of public authorities to publish certain information, and includes an explicit provision regarding the use of electronic media for the same.
 - **Part three** creates the general right of individuals to access information retained by public bodies and creates the mechanism and procedures to facilitate the grant of such access.
 - **Part four** identifies documents and types of information which are deemed exempt from either proactive publication or release otherwise pursuant to a request for access.
 - **Part five** treats with the procedures through which an applicant can seek a review of a decision of a public body to not provide access, and where necessary, to seek an appeal of the decision by an independent oversight body.
 - **Part six** provides the general framework and powers of the oversight authority to monitor implementation of Access to Public Information and provides a forum for appeals pursuant to the provisions of Part five.
 - **Part seven** outlines particular offences to the provisions of the Model Text and the penalties associated with such offences.
 - **Part eight** provides for miscellaneous considerations, including clarifying the role of the Courts and the establishment of a co-regulatory approach in the implementation of the oversight framework, and it establishes the powers to create regulations pursuant to the model text.

COMMENTARY ON SECTIONS

PART I – PRELIMINARY CLAUSES

7. **Part 1 of the Model Legislative Text (Act)** comprises five sections. The first sections provide for the preliminary clauses, including the short title and commencement provisions for the Law¹¹, as well as the general objective of the Law, to provide interpretive context to the sections thereafter presented.
8. Section 2 provides the general objectives of the model legislative text, to create a culture of transparency in the operation of public bodies, and provides a framework through which the implementation of appropriate transparency with respect to requests is overseen by an independent body. Notably, the drafting of the Model Text does not anticipate the generation of documents by the public authority/ private body in response to each request. Instead, it focuses on the provision of information through the release of “official documents” (which may be redacted in accordance with the rules of exemptions outlined in the Act.). It is the expectation

¹¹ Ed.: The author of the Explanatory Notes mainly uses the notion “Law” when referring to the Model Legislative Text (Act) on Access to Public Information (Freedom of Information).

that the requestor shall then “process” the information contained in the released official document to deduce whatever information set is sought. As such, the relationship between information, documents and official documents should be considered in the reading of the Model text. Also notable is the inclusion of paragraph (e), which suggests the proactive publication of appropriate information by public authorities. This suggestion is based on the premise that proactive disclosure would limit the need to request information from such public bodies.

9. Subsection (2) also underscores a commitment by the government to ensure that the framework is readily accessible to citizens who may wish to access the facility.

Section 3: Interpretation

10. Section 3 provides for the interpretation of particular terms in the Law¹². Of interest are the interpretations for terms such as those below.
11. The “designated authority” referred to is established, as outlined in the objectives of the Model Text, to ensure that there would be an appropriately positioned oversight agency to ensure appropriate adherence to the provisions of the Model Text and to provide a forum for preliminary appeal of decisions of public authorities.
12. “document” as it underscores 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 timely, efficient and cost-effective dissemination of information, and the ease through which these can be facilitated through the ubiquity of information and communication technology (ICT), it provides an opportunity for ICTs to assist in achieving the objectives of the Law.¹³
13. As discussed in the objectives of the Model text, the relevant authority is required primarily to provide access to information, subject to restrictions within the model text, pursuant to a request for existing information that has been generated as a course of completing its work. It is in this context that “official documents” are specifically identified for particular treatment in the Model text.
14. The issue of access to personal information is tangentially related to the broader discussion of access to all public information, but it is covered in more detail in the Privacy and Data Protection framework. In general, appropriate implementation finds the two frameworks operating in conjunction with each other, form an interlocking relationship where FOI treats with information other than that deemed personal. The definition of personal information here is thus in line with that outlined in the Data Protection model framework and is geared to focus on information that is recorded and associated with an identifiable individual. As a matter of interpretation, it is not the intention that “personal information” include information from which an individual’s identity may be deduced. This latter set of information is indeed broader than the information set under consideration by the framework.
15. The appropriate definition of “public authority” generated substantial debate throughout deliberations on the Model Text. It is required in the Policy guidelines that Access to Public Information should apply to both public authorities and to some group of private bodies that undertake public functions. The rationale for the inclusion of such a group or private bodies is based on the models of outsourcing or public-private partnerships which have developed in the

¹² Policy Building Block 1.1 “There shall be proper definition of ‘information, ‘communication’, ‘data’, ‘record’ and document’.”

¹³ Policy Building Block 1.3 “There shall be comprehensive scope of media, source of information...so that it encompasses electronic or non-electronic documents, tapes, films, sound recording, images, produced by a public party or by a private party at any time”.

provision of services to the public. In these models some aspect of processing of information and decision-making may be deferred to the partnering private body. As such, official documents related to those activities would not reside in the public authority. To ensure that this does not become a lacuna of coverage of the Access to Public Information framework, those private bodies who may have such functions and authority to perform functions deemed essential and core (inalienable) public services are deemed to fall under the rubric of this framework.

16. Further, as a matter of clarity, there should be definitive direction provided as to which private bodies are considered relevant for the purposes of the Act. It is proposed, that the remove the discretion of the private bodies and the uncertainty that it may bring, that the Minister issue an Order which will define the private bodies relevant to this law.
17. As a matter of drafting style, the term “prescribed authority” was considered to represent the cumulative group of public authorities and those private bodies to which the law would apply. This approach may not be preferred, and another form of distinction or definition may be utilised. What is essential is the recognition that some provisions of the law will apply equally to public authorities and relevant private bodies, and other provisions shall not. Examples of such are the question of publication in the Gazette of administrative and organisational information of the body. This may be applicable to the totality of a public authority but have limited application to a relevant private body. On review of the model law, the term “public/prescribed authority” refers to this cumulative category of persons. However, where “public authority” is used exclusively, such use suggests that the provision is primarily targeted to public authorities and is not applicable to the identified private bodies.¹⁴
18. The term “personal information” is included here in alignment with the definition provided in the Privacy and Data Protection Model Legislative Text. This is done to ensure consistency of interpretation between the model texts as such becomes necessary in the consideration of relevant provisions later on.

Section 4: Limitations of Applicability of the Act

19. Section 4 establishes the persons and offices to which the Law shall have no applicability. Generally, the Law is deemed not to be applicable to the Office of the Head of State and bodies which function in a judicial role, thus the exclusions of commissions of enquiry established by the Head of State, provided for in subsection (1) and the holders of judicial offices, as provided for in subsection (2) (a). However, the administrative functions associated with such offices may fall under the rubric of the Law, thus the specification of registries and/or court offices of court administration falling under the purview of the Law. It is for this reason that the exclusion provided for in subsection (2) (a) is explicitly not extended in subsection (2) (b).

Section 5: Binding the State

20. Section 5 establishes that the Bill 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.

¹⁴ Policy Building Block 2.1 “There shall be provision in law which explicitly states what is the role of “public authorities”, “prescribed authorities” and “private bodies” ...in the management of freedom of information.”
 Policy Building Block 2.2 “There shall be provision establishing that public authority in freedom of information laws should extend to any body which carries out government functions.”
 Policy Building Block 2.3 “There shall be provision establishing that, in certain instances, freedom of information shall extend to private entities once those entities are clearly providing an essential and/or permanent public service.”

PART II – GENERAL DUTY OF PUBLIC BODIES TO PUBLISH INFORMATION

21. **Part 2 of the Model Legislative Text** establishes a paradigm where certain official documents, generated in the course of the operations of a prescribed authority should be prepared for publication as a matter of course. These provisions attempt to institute a statutory obligation which targets a core presumption of how public services are offered.¹⁵

Section 6: General Obligation to Publish

22. Section 6 obliges public authorities to prepare and publish general statements in the Gazette in accordance with guidelines it prescribes. The intent of this provision is to create a channel through which interested persons may be readily appraised of the roles, functions, and most importantly, responsibilities of authorities and enterprises that administer services and products to and on behalf of the citizenry, especially with regard to functions which impact the rights of citizens or provide for the dispensing of public funds or resources.
23. The section is constructed so as to specify the distinct elements which, at a minimum, should be published.
24. Recognising that the application of this provision would need to be modified to treat with private bodies falling under the rubric of this model text, in Subsection 1A, language geared to limiting this section's applicability to the private body to only those aspects of their operation which perform the relevant public function is included.

Section 7: General Obligation to Make Documents Available.

25. Section 7 provides for the ready accessibility of the rules and guidelines that guide the operations and/or determinations of an authority or enterprise as it relates to the administration of a public service, good, resource or award. This provision provides the fundamental form of transparency to the prospective participant in a public programme, as it allows the independent scrutiny of systems and processes utilised. Not only does this section provide for the development of such official documents, but it goes further to actually instruct that such information and documents be "pushed" to the prospective user through a variety of channels.

Section 8: Use of Online Channels

26. In line with the proposed philosophy of proactive publications enshrined in sections 6 and 7, and recognising the growing ubiquity of technological platforms as a medium for information dissemination, Section 8 explicitly provides for the use of emerging channels including, but not limited to, the Internet.¹⁶
27. A common thread throughout these sections in this Part is the reaffirmation that information contained in documents deemed sensitive by this Model Law need not be subject to the obligation of pre-emptive publication or release. It is anticipated that in instances where sensitive information is included in documents earmarked for publication, such information be redacted from the document before release.

¹⁵ Policy Building Block 3.4 "The law/legal mandate shall provide for the automatic publication of certain types of information which shall be immediately made available to the public."

¹⁶ Policy Building Block 3.5 "The law/legal mandate shall provide for publication of information in electronic and in non-electronic media, in order to guarantee full accessibility."

Policy Building Block 5.8 "The law/ legal mandate shall define cost-effective strategies of publication, such as making information available via the Internet, etc."

PART III – GENERAL RIGHT OF INDIVIDUALS TO ACCESS PUBLIC INFORMATION

28. **Part 3 of the Model Legislative Text** establishes the general right of individuals to access certain official documents, a right that is integral to the core objective of the Law.

Section 9: General Right of Access

29. Section 9 provides for the general right of individuals to request official documents, or information therein from prescribed authorities, subject to considerations of exemption outlined in Part 4 of the Law.
30. Section 9, subsections (2) and (3) treat with the applicability of the general right of access with regard to information deemed confidential or otherwise exempt by Part IV of the model text.
31. First, subsection (2) provides for the application of a public interest test before the determination that a document or information within that document is deemed exempt. Where, pursuant to such a test, a document or information within a document is deemed exempt, subsection 3, which is optional, limits the period for which this exemption will be applicable.

Section 10: Considerations Associated With Certain Documents

32. Section 10 outlines the general types of information and/or official documents of a prescribed authority to which an individual has the right to either be informed of its existence and storage, or be provided access to in furtherance of the law. It is notable that this section provides a general guideline, subject to an Order issued by the relevant Minister, that documents that may otherwise be deemed exempt may be no longer classified as such after a period of twenty years. This is intended to further the objective of proactive publication of documents by public authorities.
33. Section 10 also provides that where a document is already available by another channel that the individual utilise such channel, and access thereto would not be covered by the provisions of this Law. In this way, the model legislative text seeks to adhere to the general proviso that implementation of access to public information should not be overly burdensome to the entities so obliged, and places some responsibility on the requestor to first confirm whether the information requested is already available.

Section 11: Guiding the Request for Access

34. Sections 11 and 12 provide the general procedure through which individuals may request access to particular documents. Among other things, as outlined in Section 11, this procedure places the onus on the applicant to specify sufficient information about the information or document to facilitate its ready identification. This is constructed to make it clear that the requesting party must undertake the necessary due diligence to be specific in its request so that the public (or prescribed) authority is not unduly burdened in attempting to respond to vague requests.
35. Subsection 3 is included to provide the flexibility to the public authority to establish procedures, forms and systems to effectively manage the process by which a request is made.

Section 12: Obligation to Provide Assistance to the Requesting Party

36. Notwithstanding that responsibility of the applicant outlined in Section 11, Section 12 establishes that the public (or “prescribed”) authority is still obliged to provide reasonable assistance to the applicant to allow it to make a sufficiently specific request, including such assistance as necessary if the applicant is hindered from making the request due to a disability.

As a point of interpretation, the authority is expected to assist primarily with the form of the request, and is expected to operate in good faith so as not alter the substance of the request. Other than these general guidelines specifics associated with strategies geared to increase utilisation of the FOI framework are not included and are left to the discretion of the jurisdiction to include.

Section 13: Where Information Request Needs to be Transferred Between Authorities

37. Sections 13 and 14 establish particular directions which govern the processing of a request by an applicant. Specifically, Section 13 treats with identifying the appropriate target of a request, so as to ensure timely transmission thereto. In the circumstance of a necessary transmission of a request between authorities, Section 13, subsection 2 outlines how the start of the time period is to be determined.¹⁷

Section 14: Time Constraints Associated to Response

38. Section 14 defines the timeframes within which a response to a request should be granted. Section 14, subsection (3), which is optional, provides for the public body to supply notice in instances where it requires additional time to produce documents outlined in the request. Such provision is deemed necessary where the response to the request may in fact be time-consuming. However, to ensure against public bodies continually applying this option to frustrate the objectives of the model text, a clear timeframe, beyond which extensions of the original date are not to be facilitated, is dictated.

Section 15: Options Available to the Public Authority

39. Section 15 provides the general responses available to a public/prescribed authority subject to a request – either the provision of access, the deferral of access to all or part of a document, or the refusal to grant access to documents.
40. Pursuant to these available responses, sections 16 through 21 provide for the procedures through which a decision is to be effected.

Section 16: Process by Which a Decision is Made

41. Section 16 provides the general procedure through which a prescribed authority will inform an applicant on its decision pursuant to a request. Where the decision is such that the access is facilitated, the notice shall inform the applicant of the means by which it shall be communicated. Where the decision is to deny access, the notice shall outline particulars of why the request is denied, and the recourse to which the individual may consider if he or she is dissatisfied.

Section 17: Authorities Have Some Discretion in the Prescription of Fees

42. Section 17 prescribes a framework through which fees may be applied to the access to communication of information pursuant to a request. Subsection (1) establishes the conditions for which fees are to be reasonably levied. The framework enabled by this section limits the quantum of the fee to not more than the reasonably ascribed cost to respond to the request.¹⁸

¹⁷ Policy Building Block 5.7 “The law/legal mandate shall establish timelines so that the response to requests and the provision of information are not delayed beyond reasonable time.”

¹⁸ Policy Building Block 5.9 “The law/legal mandate shall define whether the service of provision of information shall be charged, or not, inclusively where it is transferred to private bodies in the exercise of a public function.”

43. Notably, subsections (c) and (d) provide for the exemption from fees for both categories of persons and categories of documents. It is thought that such provisions would give the Minister more flexibility in establishing public policy and also provide an appropriate cross-reference with the provisions of Section 7.

Section 18: Treating With Exempt Information in the Decision

44. Section 18 provides for the appropriate course of action by prescribed authority where a document could be communicated to an applicant pursuant to a request, save for some aspects of information therein which are deemed to be exempt pursuant to Part 4, and where the prescribed authority believes that the purpose identified for the request will be served if the exempt information is excised. In the interest of disclosure, however, subsection (2) provides for the authority informing the applicant that the copy of the document to which access is provided has been redacted and the reasons for such action.

Section 19: Providing Access to Documents in Response to a Request

45. Section 19 provides for various modes, channels and formats in which the requested access can be provided, and modes, channels and formats for the presentation of official documents to the applicant. The section is structured to identify the particular modes of access that are considered appropriate.
46. Notably, while the model text provides for a broad range of options through which the information will be communicated to the applicant, subsection (2) generally obliges the authority to provide the information in the form requested by the applicant, constrained only by concerns of copyright, or the reasonable availability of the format.
47. Subsection (3) recognises that from time to time there may be constraints to the provision of access in a particular form requested by the applicant, and it provides as a default, that the same media or format used by the applicant in the request may be the best choice for reciprocal channel of communication.
48. Subsection (4) treats with considerations where the jurisdiction in issue may have more than a single official language. The approach outlined herein was thought to be the appropriate balance between accessibility and cost efficiency.

Section 20: Authority Has a Limited Option of Deferring Access

49. Sections 20 and 21 provide the general framework and limited criteria by which a prescribed authority may either defer or deny access to a document that has not been deemed exempt. With respect to the right to defer access, it is recognised that deferral may be appropriate in limited circumstances. Accordingly, Section 20 is structured as to provide for such a deferral, but to limit the applicability of this option to particular types of situations, for which some means test may be further established.
50. It is noted that section 20, subsection (3) provides for the Designated Authority to establish maximum limits of deferrals to mitigate against the abuse of this provision and provides an opportunity for the objectives of the law to be preserved. Further, this subsection provides some predictability and comfort to applicants that the reasons cited for keeping some document confidential are material.

Section 21: Authority Has an Option to Refuse Access

51. Similarly, it is notable that among the reasons identified in Section 21 for the refusal of access is the apparent abuse of the right to access by an individual where the prescribed authority can provide evidence of the harassing nature of a series of requests. This matter is deemed important enough that it is again addressed in Section 58, which treats with mitigation against this practice.

Section 22: Providing For the Delegation of Decision-making With Respect to FOI

52. For clarity on the functionary within a prescribed authority who is empowered to make the decisions, including those according to criteria outlined in Sections 20 and 21, Section 22 provides for the delegation of such responsibility from the head of the prescribed authority and or the responsible Minister (in the case of a Department of Government). This section is also crucial in the context of the provisions for internal review outlined in section 35.

PART IV – EXEMPTION OF DOCUMENTS OR INFORMATION WITHIN DOCUMENTS

53. **Part 4 of the Model Law** defines the particular documents which are deemed exempt from the general provisions of Part 3.

Section 23: Obligated Application of a Public Interest Test

54. Notably, section 23 provides for the rescission of the exempt classification on an official document subject to a “public interest” test¹⁹, and further establishes that despite the general descriptions of documents outlined in this Part, that such documents are not exempt *per se* but can only be considered exempt pursuant to the application of the same “public interest” tests²⁰. This section targets, through statutory construction, the prevailing culture of secrecy associated with the undertaking of government business, to instead replace that culture with a default culture of publication and transparency.

Sections 24 to 32: Possible Reasons For Exemption of Documents

55. Sections 24 through 32 provide descriptions of the various types of documents (or information therein) which may be deemed exempt upon application of the public interest tests²¹. These sections are constructed to specify the types of documents and information that may be exempted, or outlines the negative effect that the individual provisions seek to eliminate. Each section treats with a particular type of document or information set exclusively. Where there is an instance of optional language provided, this is in response to alternate preferences for more elaboration on a particular issue (section 29 (a)).

¹⁹ Policy Building Block 4.4 “The law/legal mandate shall state where the public interest in disclosing the information is greater than the potential harm to be caused, the information should be disclosed.”

²⁰ Policy Building Block 3.2 “The law/legal mandate shall state that no official document shall be kept confidential unless there are overriding public interest reasons to the contrary.”

Policy Building Block 4.2 “The law/mandate shall establish that in determining whether a document is exempt from disclosure, a “public interest test” be administered.”

Policy Building Block 4.3 “The law/legal mandate shall determine that documents are tested on an individual basis and are not automatically placed in an exemption class.”

²¹ Policy Building Block 4.1 “The law/legal mandate should provide for exemptions clearly and narrowly drawn, in order to avoid wide-ranging exemptions, which could defeat the purposes of freedom of information.”

These documents (or types of information) include:

- Cabinet documents, including Notes, Minutes or sub committee documents, whether draft or final;
- Documents relating to or affecting national security, defence and/or international relations
- Documents affecting the enforcement or administration of law
- Documents or information, the disclosure of which would be construed as contempt of court or contempt of the Parliament
- Documents or information related to trade secrets, business or commercial affairs of the person, or which may reasonably prejudice such affairs if disclosed;
- Documents or information affecting the national economy;

Section 33: Deference of Treatment of Personal Information to Privacy and Data Protection Framework

56. Section 33 provides appropriate provision to facilitate the protection of the privacy and personal information of persons who are not the applicant which may be compromised with the communication or grant of access to the applicant. The provision is drafted to provide for the appropriate overlap of the FOI and Privacy and Data Protection frameworks.

PART V – REVIEW OF AND APPEAL OF THE DECISIONS OF PUBLIC AUTHORITIES

57. **Part 5 of the Model Law** establishes the right of the applicant to have a forum to appeal unsatisfactory decisions of an officer of a prescribed authority. This Part, along with the dispute resolution provisions included in Part 6, provides an alternative dispute resolution framework geared to minimise the time and cost associated with judicial review actions where the applicant is dissatisfied with the response to a request for information²².
58. Sections 34 and 35 provide a framework where, in the instance where the authority to make decisions with regard to the response to or rejection of an application is delegated to an officer within the prescribed authority, the applicant may request from the head of the prescribed authority an internal review of the decision.

Section 34: Right to Internal Review Where Appropriate

59. Section 34, sub sections (1) and (2) provide for the general right of an applicant to request an internal review in response to a decision by that authority.
60. Subsection (3) restates or clarifies that a failure to give a decision on the matters outlined in subsection (1) in a reasonable time is deemed to be a refusal, and thus subject to a request for internal review.
61. Subsection (4) provides that a request for an internal review is only relevant where the decision has been made by someone other than the Head of the authority, as facilitated by Section 22.

²² Policy Building Block 5.1 “The law/legal mandate shall establish procedures for enforcement, review and appeal in connection with freedom of information.”

Section 35: Mechanics of the Internal Review

62. Section 35 outlines the valid period in which an internal review may be requested and the timeframe in which the review must be completed. Subsection (1) underscores that where an internal review is granted, the review is to be conducted by no less than head of the prescribed authority, or in the case of a Ministry, the Permanent Secretary or Minister²³. In the former case, the subsection limits the types of reasons granted which may be subject to the review of the Minister. The areas highlighted are deemed to be matters of policy that may reflect deliberation of Cabinet at large and thus require the specific consideration of the Minister.
63. Subsection (2) begins to delineate the process by which an application for internal review will be valid, outlining the timeframes within which the applicant must file for such a review.
64. Subsection (3) provides the enabling framework that guides the options for decisions of the reviewer, as well as outlines the timeframe by which the review shall be completed.

Section 36: Providing for an Appeal of an Internal Review

65. Section 36 provides for the applicant to further appeal the latter decision to the independent designated authority for further adjudication in cases where the applicant remains dissatisfied with the decision of the internal review.²⁴

PART VI – ESTABLISHING THE DESIGNATED AUTHORITY, ITS APPROPRIATE FORM AND POWERS

66. **Part 6 of the Model Law** establishes the Designated Authority. This is a critical component of an effective Access to Public Information legislative framework. The requirement for independent oversight is essential to oversee compliance by the prescribed authorities, in both the public and private sectors, and thus has to be independent of the Civil Service, allowing for appropriate distance of formal influence to provide for effective evaluation of the performance of authorities. It should be noted that while this part is drafted as if the head of this body was an individual, it is equally valid that this body is headed by a group of persons (such as a Commission or the like). The jurisdictions retain ultimate discretion in the form of governance preferred for this oversight body.
67. What is critical is that such a body is independent not only from the Political Executive, but also that there is sufficient autonomy from certain private sector interests that would fall under the umbrella of this law by the nature of the business they undertake.
68. In light of the scope of this function, to ensure access to information, oversight remains untainted by perception of bias to the Executive or any prescribed authority, a suitably situated officer must be identified to carry out this function. In fact, in many jurisdictions the role of the Authority is ascribed to similarly situated persons such as the Ombudsman. However, as shall be seen later, the need for firm provisions of enforcement that is recommended suggests that such may not be an ideal fit.

²³ Policy Building Block 5.2 “The law/legal mandate shall provide for an internal review of the original decision by a designated higher authority within the public authority.”

²⁴ Policy Building Block 3.5 “The law/legal mandate shall set forth the individual right of appeal to the independent oversight body ...upon refusal by a public authority to disclose information”

Section 37: Establishing the Designated Authority

69. Accordingly, Section 37 provides for the appointment and removal of an independent Authority in the same manner as and with similar criteria for eligibility a Parliamentary Commissioner or Ombudsman²⁵, with similar provisions for entrenchment of tenure. Further, the section ensures that the Authority has no other emolument income or other expressed obligation or allegiance which could engender the perception of bias. (These provisions are very similar to those proposed for that of the Privacy and Data Protection Commissioner).

Section 38: Definition of Tenure of the Designated Authority

70. Further, as a mechanism to maintain the integrity of the office and to provide for integrity and fairness, Section 38 establishes a maximum term of office for office holders at the Authority. This maximum term of office is longer than the election cycle, having regard to best practice.

Section 39: Protection of the Designated Authority

71. Further, in order to preserve the independence and impartiality of the Authority, Section 39 provides for protection of officers of the Authority 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 Authority for the cost of defending actions.

Section 40: Providing for the Delegation of Powers

72. As a matter of operational and organisational practicality, Section 40 empowers the Authority to delegate any of his or her investigative and enforcement powers conferred upon him by the Law to any authorized officer designated for that purpose by the Authority²⁶.

Section 41: Functions of the Designated Authority

73. As outlined in Section 41, the major functions of the Designated Authority would be to ensure compliance to the FOI legislation through:
- monitoring how the legislation is administered and conducting reviews;
 - initiating compliance investigations into the operations of prescribed authorities;
 - resolving and mediating complaints or appeals of decisions;
 - developing public education programs; and
 - promoting best practice with regard to Access to Public Information.

These general functions were compiled from reviewing best practice, as well as considering an encouragement oversight approach to the performance of the role necessary to oversee the implementation of Access to Public Information.

²⁵ Policy Building Block 5.3 “The law/legal mandate shall provide for an independent oversight and arbitration body with the power to undertake investigations on its own accord or in response to complaints, to make binding determinations, to compel parties to take action, enforce orders and impose sanctions.”

²⁶ Policy Building Block 5.4 “The law/legal mandate should provide for procedures guiding the operation of the oversight body including time limits for decisions, form of notices of appeal, of decision and delegation of power.”

Section 42: Requirement to Take an Oath of Confidentiality.

74. Section 42 requires that persons who, by virtue of the execution of functions under this Law have access to information which would be considered exempt, 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 Access to Information Law, any other enactment or as authorized by the order of a Court.

Section 43: Oversight Powers of the Authority

75. Sections 43 empowers the Authority as a regulator for the purpose of carrying out its functions, including the power to do all such acts as appear to it to be requisite, advantageous or convenient for, or in connection with the carrying out of these functions, including the power to investigate the operations of a prescribed authority on his own initiation or in response to a complaint.

Section 44: Power of the Authority to Obtain Particular Information

76. In accordance with the previous section, Section 44 empowers the Authority to obtain information about documentation, processing and security of data, and, *inter alia*, to request that a person furnishes to it in writing in the time specified access to specified information.
77. Subsection (1) introduces the mechanism of inquiry and the information notice, while subsection (2) obliges relevant authorities to respond truthfully to such a notice once issued.

Section 45: Contents of the Information Notice

78. Section 45 elaborates on the information notice, its form and content, and subsection (2) prescribes that the timeframe by which a response is expected should be included in such a notice.

Section 46: Penalty for failure to respond to the information notice

79. Section 46 subsections (1) and (2) reinforces the obligation of the prescribed Authority to respond to the information notice, and to do so truthfully.
80. Subsection (3) prescribes a failure to respond to an information notice by the Authority, or the act of wilfully responding falsely, as criminal offences.
81. Subsection (4) established a reasonable defence to the offence established by subsection (3)
82. Sections 47 through 52 establish the appropriate process by which the Authority may undertake an audit or investigation, including the receipt of a complaint from an individual, the subsequent notification to the prescribed Authority 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).

Section 47: Designated Authority to Act on Complaints

83. Section 47 provides for the Designated Authority's obligation to act in particular fashions on receipt of a complaint. The obligations include that of undertaking an investigation and notifying the complainant of the outcome of that investigation in a reasonable time.

Section 48: Form of Complaint

84. Section 48 outlines the general form to which a complaint must adhere once lodged.

Section 49: Process of Initiating an Investigation

85. Section 49 outlines the process the Designated Authority must undertake in engaging the public/prescribed Authority subject to a complaint. The mechanism proposed--the Notice of Investigation--must be served on the head of the public/prescribed Authority prior to the beginning of an investigation.

Section 50: General Powers to Undertake Searches, and Effect Seizure

86. Section 50 provides the Designated Authority with the general authorisation to enter premises of a public/prescribed authority, 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 Designated Authority should be accompanied by a police officer.

Section 51: Adherence to Principles of Exemption

87. Section 51 reinforces that earlier provisions of particular documents being exempt from processing under this law are similarly applicable in the instance of search and seizure.

Section 52: Conduct of Investigations

88. Section 52 provides general guidance on how the Designated Authority shall manage investigations. Subsection (2) provides for both parties to have the opportunity to present their case to the Designated Authority where there are hearings being undertaken to further an investigation. Further elaborations on the process are deferred to subsidiary regulations and/or rules of proceedings.

Section 53: The Enforcement Notice

89. Sections 53 establishes the mechanism by which the Authority may issue directions to prescribed authority deemed to operating in a manner not consistent with the Law. Prescribed authorities are herein obliged to respond or comply with instruction within the mechanism, the enforcement notice, or be deemed to be in breach of the Law, facing sanctions for having committed a criminal offence.

Section 54: The form and Content of the Enforcement Notice

90. Section 54 outlines the form and contents of the enforcement notice. Subsection (1) outlines that the notice should specify how the prescribed authority is deemed to be in breach, specify action that is required to be undertaken to treat with the breach, and in accordance with transparency, inform the prescribed authority of its right to appeal the enforcement notice. Subsection (2) underscores that the time by which the prescribed authority is to comply with the notice should be included therein.
91. Subsection (4) provides for the Designated Authority to withdraw an enforcement notice should such withdrawal become necessary.

Section 55: Complying with the Enforcement Notice.

92. Section 55 reinforces that the prescribed authority is obliged to act in accordance with the guidance of the enforcement notice, subject to rulings of the Courts. Subsection (2) establishes it an offence to fail to meet this obligation.

PART VII – ESTABLISHING OFFENCES AND PENALTIES FOR BREACH OF PROVISIONS

93. **Part 7 of the Model Law** outlines the criminal offences associated with the breach of particular provisions of the Law^{27, 28}.

Section 56: Offence to Breach Record Management Guidelines

94. Section 56 defines as a criminal offence the wilful breach of the record management guidelines established by the Minister in Section 61. This is intended to reinforce the import given to the adherence to record management best practice as a cornerstone in assuring accountability and operational continuity in the public sector. Further, this section defines as a particular criminal offence any such breach of record management that is deemed to be pursuant to a request to access official documents. It is intended that the penalty for the breach of the latter will be more punitive as it represents a deliberate attempt to falsify records and suppress information that redounds to the public good.

Section 57: Offence to Obstruct the Actions of the Designated Authority

95. Section 57 expands on treating with the general practice that may be deemed to be obstruction to the actions of the Designated Authority or his agents. Any such action on the part of any person can be deemed a serious action against the objectives of this Law and the ultimate objectives of enhanced transparency and thus increased public confidence. Accordingly, any such action is considered a criminal offence, and the penalty should so reflect.

Section 58: Offence to Mislead the Designated Authority

96. Similarly, Section 58 treats with persons who are deemed to have misled the Designated Authority, or who have been deemed to have abused the rights conferred by Part 5 of the Law. The offence created is geared to be a disincentive to the vexatious abuse of these empowering provisions which would otherwise undermine the operational viability of the prescribed authority, the Designated Authority or both.

Section 59: Offence to Breach Oath of Confidentiality

97. Section 59 seeks to treat with persons who breach oaths of confidentiality entered into in undertaking functions within the Designated Authority. This is geared to limit such occurrences and ensure the continued public trust in the Authority.

²⁷ Policy Building Block 5.1 “sic”

²⁸ Policy Building Block 5.10 “The law/legal mandate shall establish sanctions for the failure to comply with duties and obligations relating to freedom of information, in order to foster its compliance.”

Section 60: Establishing Whistleblower Protection

98. Section 60 provides protection for persons who, while within the employ of a prescribed authority and 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 prescribed authority²⁹. In conjunction with this protection is the statutory obligation of the Designated Authority to establish anonymous channels by which persons may in good faith release information on wrong-doing. 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. This section also identifies a breach of the whistleblower protection as a criminal offence.

PART VIII – GENERAL PROVISIONS TO FACILITATE IMPLEMENTATION OF THE FRAMEWORK

99. **Part 8 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 61: Minister to Establish Guidelines for Record Keeping

100. Appropriate systems of record keeping, storage and disposal are fundamental to the ready implementation of the later provisions of this Law. Accordingly, section 61 provides for the establishment, in statute, of a dual responsibility:- that of the relevant Minister of government to establish such standards, rules and guidelines that encourage and enshrine best practice in record management, and that of the public authorities, and applicable quasi-public and private bodies to effect systems that will be in compliance with these guidelines³⁰. In this regard, the relevant Minister may gain guidance from parties, including in particular the National Archives of the Government in the development and establishment of such guidelines and rules. Pursuant to both these obligations, the section also provides for the oversight of the implementation of this system by the Designated Authority.

²⁹ Policy Building Block 6.1 “The law/legal mandate shall establish that individuals be protected from any legal, administrative or employment-related sanctions for releasing information of wrong doing once they acted in good faith and in reasonable belief that the information was substantially true and disclosed evidence of wrong doing, as the inclusion of whistle blower protection is an indication of a government’s willingness to subject itself to legitimate scrutiny.”

Policy Building Block 6.2 “The law/legal mandate shall also establish anonymous channels for denouncement, in order to maximize chances of capturing report on wrong-doings.”

³⁰ Policy Building Block 2.4 “There shall be provision for the production and enforcement of technical standards designed to foster freedom of information.”

Policy Building Block 3.6 “The law/legal mandate shall provide for appropriate standards of update, storage and discard of information.”

Policy Building Block 3.7 “The law/legal mandate shall determine that the management of freedom of information be guided by the objectives of security, efficiency, effectiveness and user-friendly records management.”

Section 62: Development of Codes of Conduct

101. Recognising that the demands on prescribed authorities will differ, the Law defers further, more detailed directions to a co-regulatory approach proposed in Section 62. The development of codes of practice will encourage the establishment of industry-led, but Authority-facilitated, guidelines which will better fit the modalities of their operations without becoming unnecessarily burdensome.³¹

Section 63: Correction of Personal Information

102. Section 63 works in conjunction with Section 33 to provide guidance on the interaction of Freedom of Information and Privacy and Data Protection legislative frameworks.

Section 64: Role of the Courts

103. Section 64 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 Authority³². 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.

Section 65: Designated Authority to Report Annually to the Legislature

104. Section 65 provides for the Designated Authority to annually report to the Parliament on the performance of the wider Government and relevant bodies in adherence to the Access to Information practices. This section also provides statutory weight to a proposed system by which Ministers of government are obliged to provide necessary assistance, or to forward required information to the Authority in furtherance of the preparation and submission of the annual report.

Section 66: Responsibility of Minister to Enact Regulations

105. Section 66 provides a general enabling provision through which the relevant Minister may enact Regulations necessary to effect or elaborate on particular provisions throughout the Law³³.

³¹ Policy Building Block 2.5 “There shall be provision recognising co and self regulation in certain sectors or markets of activities.”

³² Policy Building Block 5.6 “The law/legal mandate shall establish that both the applicant and the public authority shall have a right of appeal to the Courts against decisions of the oversight body.”

³³ Policy Building Block 3.8 “The law/legal mandate shall define guidelines to be followed in the selection of search or filter mechanisms associated with availability of information of public interest.”

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 ³⁴	J Paul
PRESCOD	Kwesi

³⁴ 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

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

HIPCAR Consultants Participating in the Workshop

Last Name	First Name
GERCKE	Marco
MORGAN ³⁵	J Paul
PRESCOD	Kwesi

³⁵ Workshop Chairperson.

