



# THE OFFICE OF THE Data Protection Commissioner



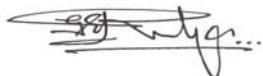
# Annual Report 2009

**The Honorable Hubert A. Ingraham  
Prime Minister & Minister of Finance  
Cecil V. Wallace-Whitfield Centre  
Cable Beach,  
P.O. Box N-3017  
Nassau, N.P.,  
The Bahamas**

Dear Prime Minister,

In compliance with Section 21 of the Data Protection (Privacy of Personal Information) Act, 2003, I am pleased to submit to you, for presentation to Parliament, the third Annual Report on the activities of the Office of the Data Protection Commissioner for the reporting year ended December 31<sup>st</sup> 2009.

Yours faithfully,



George E. Rodgers  
Data Protection Commissioner

10<sup>th</sup> February, 2010

## **What is Data Protection?**

Data Protection is the safeguarding of the privacy rights of individuals in relation to the processing of personal information. The Data Protection (Privacy of Personal Information) Act, 2003 (“The Data Protection Act”) places responsibilities on those persons processing personal information, and confers rights upon the individuals who are the subject of that information. The Data Protection Act also sets out the legal framework for the collection, use and disclosure of personal information that is consistent with international principles recognized by the Council of Europe, [The European Union (EU)] and the Organization for Economic Co-operation and Development (OECD), and the United Nations (UN).

From our point of view, the key principle of data protection is that living individuals should be able to control how personal information about them is used, with or without their consent.

“Privacy is not rocket science. It really is a simple notion about respect, choice and common sense. It is about balance; balance between the right of an individual and collective society needs.”

*(Ms. Karen Curtis, Privacy Commissioner of Australia.)*

## **ABBREVIATIONS**

BGOL	- Bahamas Government Online
COB	- College of The Bahamas
CCTV	- Closed Circuit Television
DPA	- Data Protection Act
EU	- European Union
ODPC	- Office of the Data Protection Commissioner
OECD	- Organization for Economic Cooperation and Development
TIEAs	- Tax Information Exchange Agreements
TSA	- Transportation Security Administration
UK	- United Kingdom
UN	- United Nations
USA	- United States of America

## CONTENTS

Forward.....	6
Commissioner's Statement.....	8
Important Terminology in the Data Protection Act.....	10
Data Protection A Quick Guide.....	11
Data Protection Principles and their Application.....	12
Data Protection at Work .....	14
Duties of the Commissioner.....	19
Powers of the Commissioner.....	20
Strategic Plan 2010-2012 – Appendix 1.....	21
Schedule of Agency Visits and/or Presentations – Appendix 2.....	26
Tip of the Month- Appendix 3.....	27
Organization by Functions – Appendix 4.....	28
Financial Statements – Appendix 5.....	31
Contacts – Back Page	

# **FORWARD**

This is my third report as Data Protection Commissioner for The Bahamas and it covers the year 2009.

The Data Protection (Privacy of Personal Information) Act, 2003 (DPA) came into force on April 2<sup>nd</sup> 2007, subsequent to the establishment of the Office of the Data Protection Commissioner (ODPC) in October 2006. In 2003, the DPA was accompanied by the Computer Misuse Act and the Electronic Communications and Transactions Act which together augment the mandate of the DPA which gives citizens important rights including the right to know what information is held about them and the right to correct information that is wrong. The DPA helps to protect the interest of individuals by obliging both the private and the public sectors to manage the personal information they hold in an appropriate way that is consistent with the rights of the data subject as provided by law.

As a Corporation sole, the Commissioner is independent in the performance of his duties. By law he is appointed in writing by the Governor General on the advice of the Prime Minister after consultation with the Leader of the Opposition. The Commissioner has responsibility for:-

- Administering and enforcing the provisions of the DPA.
- Promoting the observance of good practice methods by Data Controllers within the requirements of the DPA
- Influencing thinking on privacy and processing of personal information matters on a local and global basis.
- Discharging as the national supervisory authority, various functions relating to or arising from any international obligations The Bahamas may have or is seeking to be a party to, in connection with data protection.

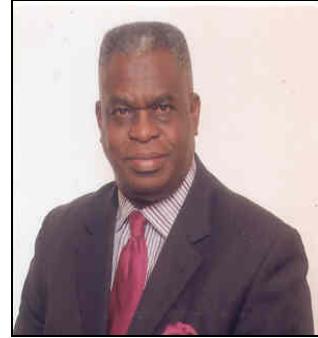
Privacy is a large component of human rights. As a member of the global village Bahamian authorities are becoming more aware of pressure being

placed on that human right by the need to protect individuals against the background of increasing security considerations. This is best demonstrated by the fallout from the Christmas Day attempt to blow up an airplane over Detroit in the United States of America (USA).

Consequently, the challenge to protect our fundamental privacy rights becomes more vivid as we seek to ensure that the various principles of data protection and human dignity in life, are maintained through the use of best practices in the field as they become operable.

## **Commissioner's Statement**

At the close of this my third year as Data Protection Commissioner, I am pleased to present the 2009 report, although I am obliged to refine my approach and methods of advancing the mandate of data protection in The Bahamas. Promoting data protection (or privacy) is challenging in normal times, but because 2009 was difficult with budget constraints, and to a larger extent the reluctance of our citizens to formally register their complaints, I plan to redouble our focus on public awareness of and compliance with the provisions of the DPA.



Consequently, I have introduced a three year Strategic Plan covering the period 2010 - 2012 to chart the way forward (see Appendix 1 for the outline of this plan).

Regrettably, our **website** statistics (on the number and subject of hits") were inadvertently lost during an upgrade of the Government's broad band network, rendering the statistics inaccessible for the year. I have taken steps to ensure this does not recur.

Again complaints and/or queries have been minimal with five (5) complaints and twenty two (22) queries being received. This compares with three (3) complaints and twenty (20) queries noted in 2008. In 2009 I was able to visit eighteen (18) agencies/institutions interacting with three hundred and four (304) individuals in the process (prior year twenty five (25) and four hundred and seventy three (473) respectively). These visits included two prominent service clubs in our community and as a result of these visits I detected a need for the brochure "Questions for your Business" which was produced in response thereto, and is now available for distribution.

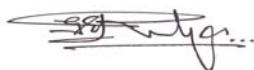
The 31<sup>st</sup> International Conference of Data Protection and Privacy Commissioners, was held in Madrid, Spain, during the first week on November, 2009. I was honored to represent The Bahamas at this event. This conference is the largest forum dedicated to privacy (data protection) in the world and every year, it brings together data protection authorities from

every continent, as well as the public, business and community sectors. There were some one thousand and sixty (1060) participants at the conference from eighty three (83) countries.

“Privacy: Today is Tomorrow” was the theme of this year’s conference through which the host country (Spain) introduced its premier resolution in the form of a joint proposal for a Draft of “International Standards on the Protection of Personal Data and Privacy.” This document was the collaborative effort of the privacy authorities from fifty (50) countries and seeks to reflect the many approaches that the protection of this right allows by integrating legislations on five (5) continents. Details of this resolution and others may be found at [www.privacyconference2009.org](http://www.privacyconference2009.org).

The need to gain more experience in Case Management (i.e. formal complaints) continues to retard our ability to progress a primary objective of any data protection authority. This involves making application to the European Commission (EU) for an assessment of The Bahamas’ data protection regime with a view to satisfying the EU adequacy test for transborder flows. Fortunately for The Bahamas, however, was the enactment of data protection legislation which enhanced our negotiating capacity for various Tax Information Exchange Agreements (TIEAs) that have been concluded in recent times. I am obliged to keep this item on the front burner in an effort to advance our cause.

Finally, I take this opportunity to thank the Acting Financial Secretary, Mr. Ehurd Cunningham and Legal Advisor, Mrs. Rowena Bethel for their continued support. Special thanks to my Secretary Mrs. Sabrina Woodside and Mr. Dexter Fernander, for their unselfish help in producing this report.



George Rodgers  
Data Protection Commissioner

20<sup>th</sup> January, 2010

## **Important Terminology in the Data Protection (Privacy of Personal Information) Act, 2003**

The following terminology is used where it relates to our data protection legislation:-

<b>“Data”</b>	means information in a form in which it can be processed.
<b>“Data Controllers”</b>	means a person who (either alone or with others) determines the purposes for which and the manner in which any personal data are, or are to be processed.
<b>“Data Processor”</b>	means a person who processes personal data on behalf of a Data Controller but does not include an employee of a Data Controller who processes such data in the course of his employment.
<b>“Personal Data”</b>	means data relating to a living individual who can be identified:- (i) from the data, or (ii) from the data and other information or data in possession of the data controller.
<b>“Processing”</b>	in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data including:- (i) organization, adaptation or alteration of the information or data; (ii) retrieval, consultation or use of the information or data; (iii) transmission of data; (iv) dissemination or otherwise making available, or (v) alignment, combination, blocking, erasure or destruction of the information or data.
<b>“Data Subject”</b>	means an individual who is the subject of personal data.
<b>“Back-up Data”</b>	means data kept only for the purpose of replacing other data in the event of their being altered, lost, destroyed or damaged.

# Data Protection

# A Quick Guide

## What is the Data Protection Act?

The Data Protection (Privacy of Personal Information) Act, 2003 (DPA) seeks to strike a balance between the rights of individuals and the sometimes “competing” interests of those with legitimate reasons for using personal information. The DPA gives individuals certain rights regarding information held about them. It places obligations on Data Controllers (those who process information) while giving rights to Data Subjects (those who are the subject of that data). Personal information covers both facts and opinions about the individual.

### 1. Rights of Individuals under the DPA.

**Individuals have a number of legal rights under The Bahamas' data protection law. You can...**

- expect fair treatment from organizations in the way they obtain, keep, use and share your information;
- subject to prescribed exceptions, demand to see a copy of all information about you kept by the organization;
- stop an organization from using your details for direct marketing;
- demand that inaccurate information about you be corrected;
- demand that any information about you be deleted, if the organization has no valid reason to hold it;
- complain to the Data Protection Commissioner if you feel your data protection rights are being infringed;
- sue an organization through the courts if you have suffered damage through the mishandling of information about you.

### 2. Obligations on Data Controllers under the DPA.

**To comply with their data protection obligations Data Controllers must:**

- collect and process information fairly;
- keep it only for one or more specified, explicit and lawful purposes;
- use and disclose it only in ways compatible with these purposes;
- keep it safe and secure;
- keep it accurate, complete and up to date (except for back-up data);
- ensure that it is adequate, relevant, and not excessive;
- retain it no longer than is necessary, except for historical, statistical or research purposes;
- subject it to prescribed exceptions, give a copy of his/her personal data to any individual, on request

## **Data Protection Principles and their Application**

There are several important personal data exclusions from the provisions of the DPA. These may be found at section 5 and include:

- items kept for the purpose of safeguarding the security of The Bahamas,
- information that the person keeping the data is required by law to make available to the public,
- data kept by an individual and concerned only with the management of his personal, family or household affairs or kept for recreational purposes,
- deliberations of Parliamentary committees,
- pending civil, criminal or international legal assistance procedures.

Otherwise, under the DPA, a Data Controller shall comply with the following provisions in relation to the data kept by him:-

<b>Principles</b>	<b>Application</b>
1. Personal data must be collected by means which are lawful and fair.	To be fair, Data Controllers must not collect personal data unless:- <ul style="list-style-type: none"><li>• the information is collected for a lawful purpose that is directly related to a function or activity of the organization, and</li><li>• the collection of the information is reasonably necessary for that purpose.</li></ul> Data Controllers must NOT collect personal data by any unlawful means. In addition, the data subject should be aware of the identity of the controller and must have given his consent if the data is to be processed.
2. The data must be accurate and, where necessary, kept up to date (except in the case of back-up data)	<ul style="list-style-type: none"><li>• Recorded information must be accurate and must be revised as appropriate.</li><li>• Care must be taken, with images which could be altered over time</li></ul>
3. The data shall be kept only for one or more specified and lawful purposes.	<ul style="list-style-type: none"><li>• It must be clear what the purposes are for which the data are processed.</li><li>• Specified purposes may be those which have been notified to the Commissioner or to the individuals.</li><li>• The data must only be kept for lawful purposes.</li></ul>
4. The data shall not be used or disclosed in any manner incompatible with that purpose or purposes.	<ul style="list-style-type: none"><li>• Data must only be used in a way consistent with the purpose (s) for which they were obtained.</li><li>• Data disclosure must also be in ways consistent therewith.</li></ul>

<p>5. The data shall be adequate, relevant and not excessive in relation to that purpose or those purposes.</p>	<p>Data kept must be:</p> <ul style="list-style-type: none"> <li>• adequate in relation to the purpose (s) for which it is kept,</li> <li>• relevant in relation to the purpose (s) for which it is kept.</li> </ul> <p>Data kept must not be excessive in relation to the purpose (s) for which it is kept.</p>
<p>6. The data shall not be kept for longer than is necessary, except in the case of personal data kept for historical, statistical, or research purposes.</p>	<ul style="list-style-type: none"> <li>• There should be a defined policy on retention periods for all items of personal data kept.</li> <li>• The retention policy and/or procedures should be revised regularly by management and staff to ensure that they remain consistent with the requirements of the DPA.</li> </ul>
<p>7. Appropriate security measures shall be taken against unauthorized access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction.</p>	<ul style="list-style-type: none"> <li>• Access to data restricted to authorized persons only.</li> <li>• Computer systems should be protected.</li> <li>• Adequate back-up procedures should be in place.</li> <li>• Staff should be aware of security measures in place to protect stored data.</li> <li>• Premises and equipment should be secured when unoccupied.</li> <li>• Alteration or amendments to data must be properly authorized and confirmed.</li> </ul>
<p>8. The Commissioner may prohibit the transfer of personal data outside the country where there is failure to provide protection either by contract or otherwise equivalent to that provided under the DPA</p>	<p>Section 17 of the DPA provides full details of prohibition.</p>

# **Data Protection at Work**

## **Public Awareness Efforts**

In order for data protection (privacy) to gain traction in the Bahamas, our citizens must first become aware of the everyday threats to their privacy and in turn their wellbeing. The Commissioner has identified several of these threats but was unable to launch as vigorous a campaign as he would have liked to address these concerns because of budgetary constraints that were mandatory in 2009, one of the most economically challenged years seen in recent times.

## **Globally Recognized Privacy Threats**

- Lack of basic awareness among data controllers of their data protection obligations.
- Lack of awareness by members of the general public.
- The ever increasing call for the National Insurance (Social Security) Number by merchants/organizations who have no legitimate need for it.
- Criminals identifying the value of personal information for criminal and fraudulent use. (For example; the e-mail scam of a relative or friend in distress in a foreign country who needs urgent assistance etc.).
- The collection of ever more personal data and sharing of this data between organizations.
- Availability of excessive personal data on the Internet.
- Lack of effective measures to secure customer and employee data.
- Lack of procedures to limit access to personal data on a “need to know” basis.

- No mechanism for ensuring that new projects take account of the legitimate data protection expectations of the public.
- Indifference by data controllers to the reputational damage from not respecting the data protection rights of their customers.

The above has illuminated the importance of public awareness & education of data protection which the Commissioner will continue to address in the coming year and beyond. As noted earlier, formal complaints have increased from three (3) to five (5) during the year while the number of general enquiries via telephone and e-mail has also increased from twenty (20) to twenty-two (22).

### **Of the five (5) complaints received:-**

- two related to refusals to release personal information on request.
- one involved correcting information already held on file.
- another sought to encourage the Police to release a copy of a crime incident (robbery) in a timely manner, and
- the final one related to a matter involving the processing of Crown Land. However, this was redirected to the proper agency as it was outside the purview of the Data Protection Commissioner.

### **Promoting Public Education**

During 2009, the Commissioner made eighteen (18) road trips/presentations to various government agencies and/or private institutions resulting in direct interaction with three hundred and four (304) individuals in the process (prior year twenty five (25) and four hundred and seventy three (473) respectively). Although the number of persons attending was less overall, in the mix were two local service clubs through which he expects wider spin-off in-so-far-as promotion of the principles of data protection are concerned. (See Appendix 2 for more details).

The Commissioner was able to reach out to key stakeholders in the North Andros District during the month of March, 2009. Twenty four representatives from all government agencies, led by the Administrator, attended this “Information Forum” which took the form of an inter-active

discussion on the challenges which may arise out of the implementation of the DPA.

Unfortunately, with the loss of his website statistics, the Commissioner was unable to gage its effectiveness during 2009. However, he is confident that this facility continues to serve a useful purpose and will seek to have enhancements made to the website next year.

Meantime, through the “Tip of the Month” feature that is delivered via our website [www.bahamas.gov/data protection](http://www.bahamas.gov/data_protection) the Commissioner was able to discuss a range of interesting issues, (See Appendix 3). One of the most topical and ongoing issues is the soon to be worldwide use of advanced airport scanners which incorporated “Whole Body Imaging.” “Millimeter Wave Passenger Imaging Technology” is the high tech solution providing the USA Transportation Security Administration (TSA) with the use of whole body scanners to improve the ability “to detect weapons, explosives and other threat items” during the passenger screening process at selected airports. This technology employs machines that use “electromagnet waves to create pictures of energy reflected off people.” The metallic looking images show outlines of private body parts and blur passengers’ faces.

TSA testing shows the body scanners excel at finding hidden items as small as a plastic button; however it raises some privacy concerns that the machines take security too far because they can show the outline of private body parts!

To ensure privacy, the TSA has assured that the passenger imaging technology being tested has zero storage capability and images will not be printed, stored or transmitted. Once the transportation security officer has viewed the image and resolves any anomalies, the image is erased from the screen permanently. The officer is unable to print, export, store or transmit the image.

In addition to not storing, printing or transmitting the image, the transportation security officer will be viewing the image on a stand-alone machine (vs. network) that is located in a remote area from the screening process. The image will not be visible to the public, and the viewing transportation security officer will not be permitted to bring any camera into the viewing area. The transportation security officer attending to the

passenger at the machine is unable to see the image produced. The officers communicate wirelessly during the screening process.

Initial feedback is that passengers are reacting positively to the new technology. Meantime, Millimeter Wave Technology will remain voluntary for passengers; those who do not wish to receive millimeter wave screening will undergo metal detector screening and a pat-down.

Data Protection and Privacy Commissioners around the world continue to monitor this development to be able to educate their respective constituents of this and other measures which some may consider intrusive.

## **Protecting the Public**

Data Protection (Privacy) appears to be debatable when it comes to measures being undertaken to protect our security as noted above. However, privacy rights need not to be at odds with security concerns or the use of modern information technology. While it is acknowledged that technology often creates new privacy challenges (like body imaging) it is equally important to ensure that proper protocols are designed and put in place before the technology is deployed. Consequently, it is imperative that the provisions under the DPA are fully complied with.

Both public and private sectors are obliged to integrate privacy protections into their security measures seeking at all times to protect the privacy of individuals (staff and/or clients).

The Commissioner is pleased to advise that The Clearing Banks' Association Code of Conduct has been revised and additional data protection protocols have been included. It will be released to the public in early 2010.

A comprehensive set of guidance notes on the use of Closed Circuit Television (CCTV) have been completed by the Commissioner; however this is being held in abeyance while the Special Advisory Committee on CCTV completes its work on the development of a National CCTV Program. The Commissioner is a member of that Committee.

The Commissioner intends to examine the current practice of releasing details of the Electoral Register to merchants/banks/other organizations upon request. Whilst the register is for public scrutiny during a general election, it does contain a fair amount of personal information which may be used for marketing, debt collection and/or law enforcement purposes. The Data Protection Commissioner is in correspondence with the Parliamentary Commissioner in an effort to improve the protocol in this regard.

The Commissioner takes this opportunity to remind both public and private sector organizations of our community that we are in year three (3) of the five (5) year grace period which allows the continued use of existing personal information (expiry date of April, 2012) without being fully compliant with Section 31 (2) of the DPA. The section states in part that:-

“Government agencies and other bodies specified in the First Schedule may continue for a period of five years from the date of entry into force of this Act, to use and process existing files that contain personal data including sensitive personal data which were acquired in circumstances in which it is not possible to determine if such was obtained in pursuance of a legal obligation or with the consent of the data subjects.”

In any event, a concerted effort by all stakeholders should be well on the way to ensuring that personal data files are updated and/or purged to promote good data protection practices.

Finally, the ODPC is available to answer questions about your privacy issues and help you to protect your personal information, but we cannot do so if you do not seek our help.

## **DUTIES OF THE COMMISSIONER**

1. To promote the observance of good practice by Data Controllers with the requirements of the DPA.
2. To provide information to the public about the legislation, how it works, and about other matters relevant to the work of the Office.
3. To issue codes of practice for guidance as to good practice about data protection where the Commissioner considers it appropriate subject to appropriate consultation. The Commissioner is also required, in appropriate cases to encourage the preparation and dissemination of data protection codes of practice by trade associations, consider those codes submitted to him, ensure appropriate consultation and then provide an opinion on the code as to good practice.
4. Annually, to prepare and cause a report in relation to his activities under the DPA to be laid before each House of Parliament in accordance with section 21 of the DPA.
5. To investigate any contravention of the DPA. The Commissioner is required to investigate whether any contravention has occurred in relation to an individual, either of his own volition or as a result of a complaint by an individual concerned.
6. To discharge, as the national supervisory authority, various functions relating to, or arising from any international obligations The Bahamas may have or is seeking to be a party to, in connection with data protection.
7. To keep proper accounts and other records in relation to the accounts, to prepare an annual Statement of Account in the form required by the Minister, with the consent of the Minister of Finance and to send copies of that Statement of Account to the Auditor General.
8. To designate from his staff at the relevant time, someone to perform his functions during any temporary absence.
9. To perform all other functions and exercise such powers as are reasonably and legally contemplated by or necessary for giving full effect to the provisions of the DPA and for its due administration.

## POWERS OF THE COMMISSIONER

1. ***Enforcement powers\****. These include service of information notices (S.18) and enforcement notices (S.16), to enable the Commissioner to investigate and rectify instances of non-compliance with;
  - any of the data protection principles,
  - any other requirements of the DPA.
2. ***Transborder data flows\****. The Commissioner has power to issue prohibition notices, prohibiting the transfer of personal data in circumstances where the data would lose its protections under the DPA. (S.17).
3. To prosecute any offence under the DPA together with associated powers of entry and inspection in connection with the investigation of any such offence (or contravention of any of the data protection principles).

\* NB. All notices are subject to appeal to the Supreme Court under Section 24.



## Office of the Data Protection Commissioner

# Strategic Plan 2010-2012

*Appendix 1*

<b>Our Mandate:</b>  To oversee the administration and enforcement of the provision of the Data Protection (Privacy of Personal Information) Act, 2003 and within that context to protect and promote privacy.	<b>Context:</b>  The Office of the Data Protection Commissioner is established under the Data Protection (Privacy of Personal Information) Act, 2003 to: <ul style="list-style-type: none"><li>• Administer and enforce the provisions of the Act.</li><li>• Promote the observance of good practice by data controllers within the requirements of the Act. Providing advice and assistance to individuals and organizations.</li><li>• Influence thinking on privacy and processing of personal information matters on a local and global basis.</li><li>• Discharge as the national supervisory authority, various functions relating to or arising from any international obligations The Bahamas may have or is seeking to be a party to, in connection with data protection.</li></ul>
<b>Our Mission:</b>  To protect and promote the privacy rights of individuals.	

## **Our Values:**

As an agency of the Government of the Commonwealth of The Bahamas. The Office of the Data Protection Commissioner is committed to assisting with the development of The Bahamas Government online (BGOL) initiative. In particular we will:

- Demonstrate leadership in promoting and protecting privacy
- Act with independence, impartiality and integrity
- Value our public officers who promote the BGOL initiative
- Be responsive to our clients
- Work collaboratively with stakeholders.

GOALS	STRATEGIES	ACCOUNT FOR 2010 & REVIEW
<b>High Quality Results</b>	Begin the process of building a policy and strategic analysis capacity.	<ul style="list-style-type: none"><li>• Develop opportunities for collaborative work.</li><li>• Initiate a targeted research program to inform the Office's policy work and promote consideration of data protection (privacy) issues.</li></ul>
	Identify and focus our policy and analysis efforts on areas of maximum impact.	<ul style="list-style-type: none"><li>• Identify partnership opportunities to maximize our ability to advise on key policy issues.</li></ul>
	Increase our influence through quality advice and information.	<ul style="list-style-type: none"><li>• Develop standards for excellence on customer service.</li></ul>
	Educate the public on the existence of the DPA legislation.	<ul style="list-style-type: none"><li>• Engage the Media (newspapers, radio and television) to maximum benefit.</li></ul>
	Sensitize Government Agencies and the general public on the steps they need to take to comply	<ul style="list-style-type: none"><li>• Produce and distribute relevant material for publication via brochures and/or Webpage listings.</li></ul>

	with DPA provisions	
	Manage our resources effectively, flexibly and efficiently.	<ul style="list-style-type: none"> <li>• Prioritize incoming work to maximize effect.</li> <li>• Maximize the impact of our policy advice through follow-up strategies.</li> </ul>
	Encourage the citizenry to make use of the Office of the Data Protection Commissioner in solving privacy complaint issues.	<ul style="list-style-type: none"> <li>• Advertise the provisions of Section 8.</li> <li>• Provide a timely complaint resolution</li> <li>• Ensure consistency in decision making.</li> </ul>
	Seek out and examine systematic information handling issues.	<ul style="list-style-type: none"> <li>• Identify key protection issues and target systemic issues to best advantage</li> </ul>
Increased <b>awareness</b> of privacy choices and obligations within the community	<p>Communicate effectively with more targeted integrated strategies</p> <p>Harness exiting communications channels to maximize effect, especially emerging popular mediums.</p>	<ul style="list-style-type: none"> <li>• Develop and implement communication plans targeting key stakeholders like COB and high school students, government agencies and the business community.</li> </ul>
	Utilize the Media to deliver the Data Protection (Privacy) message.	<ul style="list-style-type: none"> <li>• Develop and implement a media strategy.</li> </ul>

	Ensure that materials published by the ODPC are up-to-date, accurate and targeted at identified key audiences.	<ul style="list-style-type: none"> <li>• Review content and structure of our brochures and other written material.</li> </ul>
	Ensure that the Website as the ODPC's key communication channel is up-to-date and accurate.	<ul style="list-style-type: none"> <li>• Review content and design of Website.</li> </ul>
	Develop guidance material to assist the private sector.	<ul style="list-style-type: none"> <li>• Develop appropriate training material and</li> <li>• Be prepared to participate in training initiatives in the private sector.</li> </ul>
<b>Robust Relationships</b>	Ensure that effective relationships, partnerships and networks are at the core of how we operate internally and externally	<ul style="list-style-type: none"> <li>• Identify, build and manage new relationships</li> <li>• Train and support staff to manage internal and external relationships.</li> </ul>
	Develop formal links with external parties where appropriate and useful to maximize influence and understanding.	<ul style="list-style-type: none"> <li>• Develop international linkages where warranted.</li> </ul>

<b>A confident and competent workforce</b>	<p>Attract well qualified staff where needed.</p> <p>Be committed to staff training and development; acquiring a skills base to respond to emerging issues, including new technology.</p>	<ul style="list-style-type: none"> <li>• Build a reputation to become a “preferred employer.”</li> <li>• Review career development framework for staff.</li> <li>• Promote and encourage knowledge sharing.</li> <li>• Provide training and development opportunities.</li> </ul>
--------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## **Schedule of Agency Visits and/or Presentations**

<b>Date</b>	<b>Agency</b>	<b>Number of Participants</b>
Feb. 12	Port Department	09
Feb. 19	Ministry of Lands & Local Government	03
Feb. 24	Dept. of Environmental Health Services	09
Mar. 04	North Andros District	24
Mar. 25	Dept. of Labour	09
Apr. 08	Dept. of Statistics	18
May 12	Princess Margret Hospital	78
May 20	Dept. of Social Services	22
June 10	Office of the Auditor General of The Bahamas	26
June 24	The Gaming Board	13
July 16	Bahamas Information Services	12
July 23	Dept. of Meteorology	12
	<b>NON-GOVERNMENT AGENCIES</b>	
Aug. 25	Kiwanis Club of Fort Nassau	32
Sept. 07	Rotary Club of New Providence	28
Sept. 08	First Caribbean Int'l Bank	9

December 2009

## **TIP OF THE MONTH**

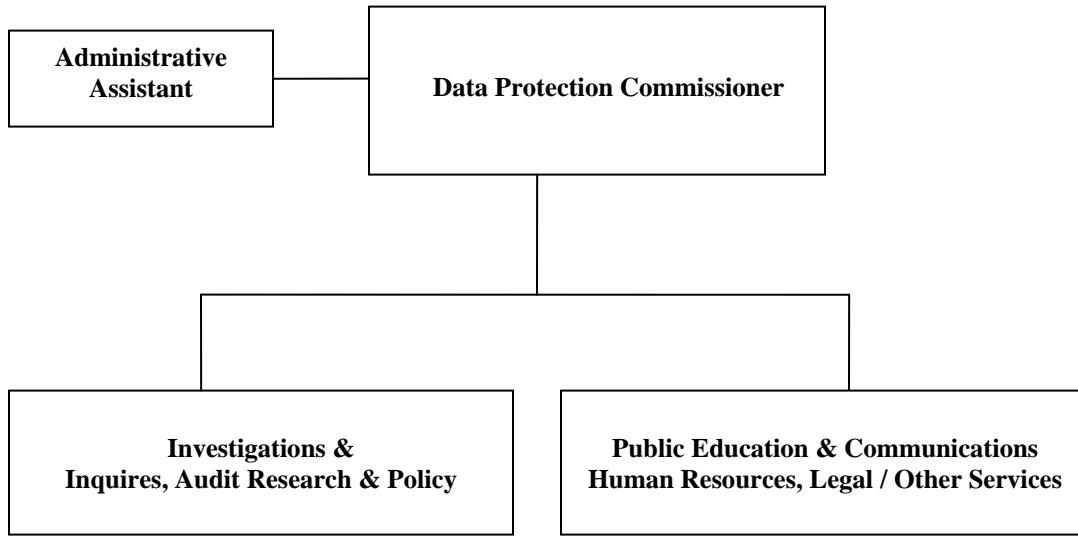
During the year the following topics were promoted through our “Tip of the Month” feature:-

- |           |                                                    |
|-----------|----------------------------------------------------|
| January   | Focus on Protecting Our Children’s Online Privacy. |
| February  | 10 Simple Ways to Protect Your Privacy.            |
| March     | The Golden Rule.                                   |
| April     | Whole Body Imaging is now a Reality!               |
| May       | Job Hunting and Data Protection.                   |
| June      | Accessing your Personal Information.               |
| July      | Computer Offences and Your Privacy.                |
| August    | Protecting our Children on the Web.                |
| September | What’s Data Protection all About?                  |
| October   | Know Your Rights under the DPA.                    |
| November  | Beware: You have a Relative in Distress!           |
| December  | Shop Smart this Christmas.                         |

The focus has been on protecting the privacy of individuals, especially the children in our society.

## **Organization by Functions**

The staff in the ODPC is comprised of the Commissioner and his Secretary (described as an “Administrative Assistant” in the below chart). The chart, however, depicts the functions of the office which are now within the purview of the Commissioner, but which may revolve into job positions/units with the growth of the activities of the ODPC. It should be noted that the ODPC is located within the premises of the Ministry of Finance and is able to call on the Legal Unit of the Ministry for advice and assistance in case of need. No staff adjustments are planned at this time.



A synopsis of the various activities and/or comments in each work category is given below:

### **Investigations and Inquiries**

- Investigating complaints received from individuals under Section 15 of the DPA.
- Establishing whether individuals have had their privacy rights violated.
- Determining whether individuals have been afforded their rights to access to their personal information.
- Where privacy rights have been violated, seek to provide redress and to ensure violations do not recur.
- Mediation and conciliation, with a view to corrective action, if necessary, are the preferred approaches to complaint solving.

- The Commissioner has the power to issue enforcement notices to compel violators to comply with the provisions of the DPA.
- There is provision under Section 24 of the Act for leave to appeal to the Court against the prohibition specified in the Notice within 21 days from the service of Notice.
- The Commissioner's office will be receptive to all privacy complaints, Section 15 (2) (a). However frivolous or vexatious complaints will be discouraged.

### **Audit Research & Policy**

- Here we will assess how well organizations comply with the provisions and spirit of the DPA.
- Compliance reviews of the function and or work of a Data Controller or a Data Processor is also the concern of this area, and the application of the Act outlined in Section 4 of the DPA.
- The Commissioner will receive, analyze and provide comments and recommendations on Data Protection issues affecting The Bahamas.
- He will also seek to ensure that privacy risks associated with specific programs and services are properly identified and that appropriate measures are taken to mitigate these risks.
- Develop a center of expertise on emerging Privacy/Data protection issues at home and abroad.
- Research trends, monitor Legislative and regulatory initiatives and provide analysis on key issues, including policies and positions that advance the position of the Privacy rights of personal information.
- Identify Legislation, new programs and emerging technologies that raise privacy concerns, providing strategic advice and policy options.
- Draft discussion and/or position papers for public consumption on issues affecting Privacy; and personal briefing material for public speeches etc.

### **Public Education & Communication**

- Promote the observance of good practice by Data Controllers within the requirements of the Act.
- Provide information to the public about the Legislation and how it works, and about relevant matters.
- Issue codes of practice for guidance as to good practice about Data Protection.
- Encourage the preparation and dissemination of Data Protection codes of practice by trade associations; consider codes submitted for review and ensure appropriate consultation, providing an opinion on the codes as to good practice.
- Discharge various functions relating to or arising from international obligations of The Bahamas, as regards Data Protection (privacy) issues.
- Plans, and implements a number of public education and communications, activities, including speaking engagements and special events, media relations, advertising, the production and dissemination of promotional and educational

material. Clearly all of the above will not fall into place immediately, but it is anticipated that the framework will evolve over time.

### **Human Resources – Legal & Other Services**

- The message must go out to Human Resource Management Personal that they are responsible for performing Data Protection functions either as a Data Controller or a Data Processor for the purposes of the Act.
- In particular, the Head of a Government Agency is deemed to be Data Controller or as the case may be, a Data Processor under Section 3 of the Act.
- Legal matters under the Act will be referred to the Legal Advisor in the Ministry of Finance.
- Other services, notably advice on finance, information technology and general administration will be sought from development partners within the Ministry of Finance.

# Financial Statements

## Receipts and Payments for the period January 1<sup>st</sup> 2009 to December 31<sup>st</sup> 2009

(Expressed in Bahamian Dollars)

### Receipts

	2009	2008
Contribution provided via the Ministry of Finance (Note 1)	140,229	\$ 111,178
<b>Total Receipts</b>	<b>140,229</b>	<b>\$111,178</b>

### Payments

Salary & Allowances (Note 2)	133,900	\$102,400
Travel & Subsistence	340	1,150
Training & Related costs	4,244	5,404
Office & Computer Equipment	200	360
Furniture & Fittings (Note 3)	-	-
Miscellaneous Expenditure	1,545	1,864
<b>Total Payments</b>	<b>140,229</b>	<b>\$111,178</b>

### Notes:-

- Contribution provided via the Ministry of Finance.** The Commissioner does not operate an independent accounting function. All expenses of the Office are met from within the resources of the Ministry of Finance. Consequently the expenses detailed in the above financial statement are of **notional value only**.

### 2. Salaries & Allowances.

- (a) The Commissioner was appointed by the Government initially for a period of three (3) years and this appointment has been extended for a further three (3) years to expire in October 2012. The figure at note (2) reflects the remuneration of the Commissioner and his staff, and includes gratuity in respect of the prior contract.
- (b) Staff other than the Commissioner, are established public officers. Presently the complement consists of the Commissioner and his Secretary.

- Furniture & Fittings.** The Commissioner maintains an office at the Ministry of Finance. No Purchases were made during 2009.

## CONTACTS



**The Office of the  
Data Protection Commissioner  
Of The Bahamas**



**Second Floor  
Cecil Wallace-Whitfield Centre,  
Cable Beach  
P. O. Box N-3017  
Nassau, Bahamas  
Tel: (242) 702-1553/ 702-1534  
E-mail: [dataprotection@bahamas.gov.bs](mailto:dataprotection@bahamas.gov.bs)  
[www.bahamas.gov.bs/dataprotection](http://www.bahamas.gov.bs/dataprotection)**