



THE OFFICE OF THE Data Protection Commissioner



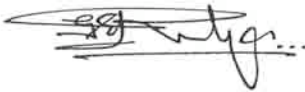
2008 Annual Report

**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 second Annual Report on the activities of the Office of the Data Protection Commissioner for the reporting year ended 31st December, 2008.

Yours faithfully,

A handwritten signature in black ink, appearing to read "George E. Rodgers", written over a horizontal line.

George E. Rodgers
Data Protection Commissioner

27th February, 2009

WHAT IS DATA PROTECTION?

Data Protection is the process of identifying and safeguarding the privacy rights of individuals in relation to the processing of personal information. The Data Protection (Privacy of Personal Information) Act, 2003 sets out the legal framework for the collection, use and disclosure of personal information consistent with internationally recognized principles established 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.

“A man without privacy is a man without dignity; the fear that Big Brother is watching and listening threatens the freedom of the individual no less than the prison bars.”

(Professor Zelman Cowen, 1969 “The Private Man” ABC Boyer Lectures).

GLOSSARY

BACO	- Bahamas Association of Compliance Officers
BGOL	- Bahamas Government On-line (Initiative)
CBB	- Central Bank of The Bahamas
CCTV	- Closed Circuit Television
DPA	- Data Protection (Privacy of Personal Information) Act, 2003
EU	- European Union
FAQs	- Frequently Asked Questions
NIB	- National Insurance Board
ODPC	- Office of the Data Protection Commissioner
OECD	- Organization for Economic Co-operation and Development
UN	- United Nations

CONTENTS

Forward	7
The Commissioner's Statement	9
Important Terminology in the Data Protection Act	11
Data Protection at a Glance	12
Data Protection Principles and their Elements	13
The Commissioner at Work	15
Duties of the Commissioner	18
Powers of the Commissioner	19
Website Statistics for the year ended 31 st December, 2008 - Appendix 1	20
Case Study – Appendix 2	21
Schedule of Agency Visits and/or Presentations - Appendix 3	23
Tip of the Month - Appendix 4	24
Organization by Functions - Appendix 5	25
Financial Statement - Appendix 6	27

FORWARD

This is my second report as Data Protection Commissioner for The Bahamas. It covers the calendar year 2008, of the operation of the Data Protection (Privacy of Personal Information) Act, 2003 (DPA).

The establishment of the Office of the Data Protection Commissioner (OPDC) in October, 2006 was a significant step forward for The Bahamas in terms of data protection legislation as it began the continual and progressive course toward becoming an open and transparent community. It is acknowledged that the field of data protection is challenging with new aspects being introduced almost daily. It is therefore more apparent that we must, as a regulatory authority and a “small state,” ensure that we are responsive and proactive.

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.

Bahamians are no doubt aware that there is an on-going Bahamas Government On-line Initiative (BGOL) designed to enhance the delivery of progress and services by making them available over the Internet. The DPA is an essential part of the Government’s E-Commerce enabling package and you will see elsewhere in this report that we have been successful in making available to the public various educational material on-line via our website www.bahamas.gov.bs/dataprotection

Our aim is to ensure that personal information that is collected on individuals is managed in a manner which ensures that fundamental privacy rights are observed and that the data is used in a manner that is consistent with the intentions of the data subject.

This is a noble challenge, made against the rapid growth seen in the use and accessibility of data compiled from the Internet, and in the process, providing fertile ground for the misuse of personal data by criminal elements in our society.

It is our task, therefore, to apply the various principles of data protection (detailed in this report) to best use and in line with best practices in this field.

COMMISSIONER'S STATEMENT

I am delighted to present my second report as Data Protection Commissioner. Following on from the successful first year of implementation of the DPA, we were pleased to see a significant number of “hits” to our website which recorded a total of 6,314 visits for the period under review. (See **Appendix 1** for a summary of the interest shown under the various sections).



I am particularly pleased with our website as it provides an accessible medium to disseminate information while helping us in fulfilling our objective of providing individuals and businesses with the information they need to be informed of their rights and responsibilities under the DPA.

Bahamians generally seem to take time to “warm up” to new initiatives, particularly where there is no perceived urgency. This has been the case with this initiative. Indeed one of the fundamental challenges I have is to encourage our citizens to step forward and let us know of the data protection issues they encounter; they must be willing to formally register their concerns so that those concerns can be properly addressed.

Consequently, complaints and/or queries have been below the level expected at this time with three (3) complaints and twenty (20) queries being received. This compares with one (1) complaint and nine (9) queries noted in the initial period. However, I was able to visit twenty-five (25) agencies/ institutions, interacting with four hundred and seventy three (473) individuals in the process (prior year 19 and 229 respectively).

Appendix 2 gives a synopsis of one of the complaints handled during the year in the form of a Case Study.

Another challenge I have is to encourage data controllers, both private and public, to begin to put in place an effective “data protection security plan” to ensure compliance with the DPA. To this end we have produced a brochure that (a) asks the question “Are you ready for Data Protection?” and (b) incorporates a “Data Protection Checklist” to help data controllers in this regard. A discussion of these two topics can be found in the “Resource Centre” of our Website www.bahamas.gov.bs/dataprotection

On the international scene, during the month of October, 2008, I was fortunate to represent The Bahamas at the 30th International Conference of Data Protection and Privacy Commissioners that was held in the prestigious Hemicycle of the Council of Europe, Strasbourg, France. The theme of the Conference was “Protecting Privacy in a Borderless World.” The Conference was jointly sponsored by the French and German Data Protection Authorities and it sought to identify “major challenges arising from the fact that privacy in an international context is subject to powerful technological, political, legal and economic developments.” A variety of interesting topics were examined leading to the production of several key resolutions. From our perspective the resolution on the protection of children was paramount and this has been reproduced on our Website in the “Media Centre” Category. The full cadre of resolutions may be found at <http://www.privacyconference2008.org>

The need to gain more experience in Case Management (i.e. complaints) has retarded 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. I will continue to keep this item on the front burner in an effort to advance our cause.

Finally, I am obliged, once again to thank the recently retired Financial Secretary, Mrs. Ruth Millar and Legal Advisor, Mrs. Rowena Bethel for their continued support. Special thanks to my Secretary Mrs. Sabrina Fowler-Woodside and Mr. Dexter Fernander, for their unselfish help in producing this report.



George E. Rodgers
Data Protection Commissioner

27th February, 2009

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:-

- “Data”** means information in a form in which it can be processed.
- “Data Controllers”** 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.
- “Data Processor”** 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.
- “Personal Data”** 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.
- “Processing”** 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.
- “Data Subject”** means an individual who is the subject of personal data.
- “Back-up Data”** means data kept only for the purpose of replacing other data in the event of their being altered, lost, destroyed or damaged.

DATA PROTECTION AT A GLANCE

The 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;
- 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;
- give a copy of his/her personal data to any individual, on request.

DATA PROTECTION PRINCIPLES AND THEIR ELEMENTS

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:-

Principles	Elements
1. Personal data must be collected by means which are lawful and fair.	<p>To be fair, Data Controllers must not collect personal data unless:-</p> <ul style="list-style-type: none"> • the information is collected for a lawful purpose that is directly related to a function or activity of the organization, and • the collection of the information is reasonably necessary for that purpose. <p>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.</p>
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"> • Recorded information must be accurate and must be revised as appropriate. • Exercise care with images (example photos) which could be altered over time.
3. The data shall be kept only for one or more specified and lawful purposes.	<ul style="list-style-type: none"> • It must be clear about the purposes for which the data are processed. • Specified purposes may be those which have been notified to the Commissioner or to the individuals. • The data must only be kept for lawful purposes.
4. The data shall not be used or disclosed in any manner incompatible with that purpose or purposes.	<ul style="list-style-type: none"> • Data must only be used in a way consistent with the purpose(s) for which they were obtained. • Data disclosure must also be in ways consistent therewith.

Principles	Elements
5. The data shall be adequate, relevant and not excessive in relation to that purpose or those purposes.	<p>Data kept must be:</p> <ul style="list-style-type: none"> • adequate in relation to the purpose(s) for which it is kept, • relevant in relation to the purpose(s) for which it is kept. <p>Data kept must not be excessive in relation to the purpose (s) for which it is kept.</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.	<ul style="list-style-type: none"> • There should be a defined policy on retention periods for all items of personal data kept. • 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.
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.	<ul style="list-style-type: none"> • Access to data restricted to authorized persons only. • Computer systems should be protected. • Adequate back-up procedures should be in place. • Staff should be aware of security measures in place to protect stored data. • Premises and equipment should be secured when unoccupied. • Alteration or amendments to data must be properly authorized and confirmed.
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.	Section 17 of the DPA provides full details of prohibition.

THE COMMISSIONER AT WORK

Promoting Public Awareness

During the first year of operation the Commissioner realized that promoting general awareness of Data Protection will be one of his greatest challenges. This has been proven correct and must now be regarded as his most important work goal in both the public and private sectors next year. As noted earlier, formal complaints (3) have been negligible and while the number of general enquiries via telephone and e-mail have increased from nine (9) to twenty (20), this was also below the anticipated demand.

Visits/presentations to various government agencies and/or private institutions placed the Commissioner in contact with a creditable four hundred and seventy three (473) individuals; up from (229) last year. (See **Appendix 3** for details). This process made clear the need to repeat the question that was the subject of the Tip of the Month for March, 2008:

“Do you have a Data Protection Problem?”

You might have a data protection problem if any of the following apply to you:

1. You have been denied any of your rights, including your rights to see the personal information an organization holds about you.
2. Personal information about you is used, held or disclosed:
 - Unfairly
 - For a reason that is not the one it was collected for, or
 - Without proper security.
3. Personal information about you is:
 - Inadequate, irrelevant or excessive
 - Inaccurate or out of date, or
 - Kept for longer than is necessary.

The above goes to the core of the principles of data protection with particular reference to Section 8 of the DPA which deals with access to personal information. The previous pages on “Data Protection at a Glance” and “Data Protection Principles and their Elements” provide further input in this regard.

Promoting Public Education

You will note from **Appendix 3** that during the first half of the year the Commissioner was able to travel to Grand Bahama, Abaco, and Exuma to appraise those islands about the provisions of the DPA. Each presentation was arranged to accommodate representatives from all government agencies. Some private sector individuals were also invited to attend; the response was good.

While in Exuma, the Commissioner was featured on the Exuma Radio Station “The Breeze 98.3” promoting awareness of the DPA and encouraging citizens to take advantage of the services extended by the ODPC.

In addition the Commissioner was a guest on the Television Show “Let’s talk About” with host Steve McKinney. This programme aired on ZNS TV on several occasions. The Commissioner was also a guest speaker at the Annual General Meeting of the Bahamas Association of Compliance Officers (BACO). This was followed with another opportunity to attend an Anti-Money Laundering Seminar that was promoted by BACO where the Commissioner addressed the topic “Data Protection and Confidentiality and the Role of the Data Protection Commissioner.” An overview of the address can be found at the “Media Centre” of our Website www.bahamas.gov.bs/dataprotection

Additions have been made to the Frequently Asked Questions (FAQs) feature on the Webpage in the “Resource Centre under the sub-heading “Everyday Privacy Questions.” These seek to address more of the practical data protection issues.

The Commissioner has also developed a monthly educational tool called “Tip of the Month” that is delivered via our Website www.bahamas.gov.bs/dataprotection. It seeks to highlight a topical issue each month and has been a medium that is beginning to evoke enquiries.

A full list of the subjects discussed during the year may be found at **Appendix 4** Educational Brochures on Data Protection on a range of topics have been produced including:

- What you need to know and how it affects what you do!
- Identity Theft.
- Why Complain?
- Are you ready for Data Protection?
- Managing a Data Security Breach.
- Social Networking and Protecting our Children.

These are available at the ODPC upon request.

Protecting the Public

Identity theft is the unauthorized collection and use of your personal information usually for criminal purposes. In this regard, the Commissioner is concerned about the widespread use of the National Insurance Board (NIB) number as a means of identification. Consequently, discussions are on-going with several government agencies in an effort to curb this practice, thereby limiting its potential for misuse by identity thieves.

The brochure “Managing a Data Security Breach” brings life to the principle that personal data must be properly secured. It identifies what can trigger a security breach and discusses the elements needed in a Breach Management Plan which includes:-

- containment and recovery
- assessment of on-going risk
- notification of breach and
- evaluation and response

Of all the brochures produced thus far “Social Networking and Protecting our Children” is the most topical one. It seeks to educate parents, guardians and children about social networking and create a sense of awareness of the possible dangers to children who are users of the Internet. It is acknowledged that sites such as **Facebook** and **Myspace** are widely used for social networking, however, while children (and adults) are able to increase their circle of friends, they must also be able to protect themselves from exposure to people with less than friendly intentions.

There is a need to examine the current Code of Conduct of the clearing Bank’s Association in concert with the Central Bank of The Bahamas (CBB) with regard to its commitment to protect the personal data of its customers. The Commissioner will work with the CBB to encourage/develop a good model to the best advantage of our citizens.

Closed Circuit Television (CCTV) is a method of surveillance that will undoubtedly impact upon the privacy of our citizens in the immediate future. The Commissioner is cognizant of this fact and expects to issue a comprehensive set of guidance notes on the use of CCTV before the end of June 2009.

Finally, the Commissioner takes this opportunity to remind both public and private sector organizations of our community that we are in year two (2) of the five (5) year grace period which allows the continued use of existing personal information (expiry date 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 underway to ensure personal data files are updated and/or purged to promote good data protection practices.

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 among 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

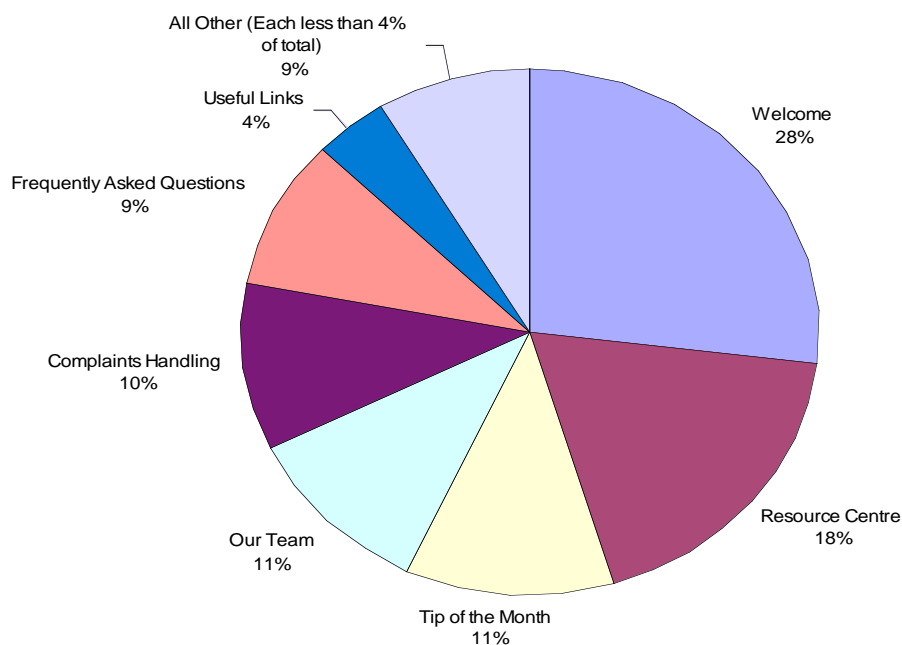
1. ***Enforcement powers****. These include service of information notices (S.18) and enforcement notices (S.16), to enable the Commissioner to investigate and rectify instances of non-compliance with:
 - any of the data protection principles
 - any other requirements of the DPA.
2. ***Transborder data 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.**

Website Statistics for the year ended 31st December, 2008

Hits total 6314 from website launch date 10th December 2007 to 31st December 2008. We are pleased with the level of activity and continue to promote the site at every opportunity.

Area	No. of Hits	Percentage
Welcome	1,705	28
Resource Centre	1,162	18
Tip of the Month	726	11
Our Team	692	11
Complaints Handling	636	10
Frequently Asked Questions	591	9
Useful Links	264	4
All Other (Each less than 4% of total)	538	9
Total	6,314	100



The above table records all the areas which have produced a better than 9% level of activity except in the case of “Useful Links” which indicates a 4% usage.

This is important because it indicates that we are beginning to encourage other entities to cross-reference us as well.

Note that while the “Complaint Handling” section received a good 10% of the visits, the Bahamian public remains somewhat reticent when it comes to actually lodging a formal complaint. Only further development in self-confidence will change this laissez-faire attitude.

CASE STUDY

Substance of Complaint:

An educational institution:

- Refused to give access to personal information;
- Refused to amend its records upon written request to do so;
- Disclosed and/or requested personal information to/from a third party without proper authorization

Governing Data Protection Principles (See Page7):

Personal information must:-

- be collected by means which are lawful and fair
- be accurate and kept up-to-date
- not be used or disclosed in any manner incompatible with the intended purpose
- be adequate, relevant and not excessive

Facts:

Parents of a student (the complainant) formally asked the educational institution (the respondent) for a copy of their child's personal records. This was repeatedly refused and in subsequent voluminous correspondence it transpired that other infractions were being perpetrated. This evoked other elements of the above complaint made against the respondent. The complainant sought legal counsel who also had difficulty in obtaining the co-operation of the respondent, even after appraising the respondent of the provisions of the DPA. Eventually, the respondent, perhaps on the advice of their own independent counsel, released the requested records to the complainant.

Subsequently, the complainant lodged a formal complaint with the Office of the Data Protection Commissioner (ODPC) in an effort to confirm their rights under the law and to recoup or receive some compensation for the legal costs they were obliged to incur.

Issues:

Section 8 of the DPA provides that an individual (in this case the parents of a minor) may access personal information a data controller (the respondent) holds about the student unless certain exceptions apply. These exceptions address a range of situations including where providing access may have an unreasonable impact on the privacy of others. Section 9 details these exceptions, none of which were applicable to this case.

The respondent's objections were somewhat odd as their own in-house policy promoted openness and transparency. In their favour, the complaint's failure to provide sensitive information at the time of the child's registration had a negative impact in the process. Meantime the respondent was unaccustomed to having their decisions challenged.

Outcome:

The Commissioner investigated the complaint and determined that in the final analysis it was **well-founded** and he communicated his decision to the relevant parties.

He pointed out, however, that:

- The complainant had to bear part of the blame because of the omission of sensitive information at the beginning of the relationship with the respondent.
- At the time the complaint was lodged with the ODPC, Section 8 of the DPA (provisions for access) was in its “grace period” and was therefore not fully enforceable.
- The respondent had already seen the wisdom of providing the complainant with the records requested.
- The subject student had already been relocated to a new institution with no apparent adverse affect.

Having regard to all circumstances of the case, the Commissioner declined to award compensation in the case. He did however, suggest to the parties concerned that they should meet with a view to mitigating the matter of legal costs.

Finally, the parties were advised of their right to appeal the decision of the Commissioner via the Courts under Subsection (1) of Section 15 of the DPA.

Lessons Learned:

- Proper personal information handling practices (policies, procedures, third party disclosure) are necessary to protect personal information and provide individuals with access to their information.
- Personalities and/or emotion should be left out of the decision making process, when it comes to fulfilling obligations under the DPA.

SCHEDULE OF AGENCY VISITS AND/OR PRESENTATIONS

Date	Agency	Number of Participants
Feb. 18	Grand Bahama Island (Consortium of Government Agencies)	57
April 09	Abaco Island (Consortium of Government Agencies)	25
April 10	Bahamas Information Services: Recording for “Let’s Talk About” TV Show	03
May 06	Passport Office	44
May 06	Ministry of Foreign Affairs	35
May 21	Post Office Department	16
May 22	Ministry of National Security	06
May 27	Ministry of Health & Social Development	06
June 17	Exuma Island (Consortium of Government Agencies)	24
June 24	Bahamas Customs Department	06
Aug. 28	Ministry of Education	30
Sept. 08	Agriculture & Marine Resources	08
Sept. 16	Parliamentary Registration Dept.	07
Sept. 18	Broadcasting Corporation	10
Sept. 23	College of The Bahamas	13
Oct. 08	Bahamasair Holdings Ltd.	04
Oct. 09	Treasury Department	17
Nov. 20	Department of Trade	07
Dec. 04	Ministry of Finance et al	32
	Non-Government Agencies	
Feb. 12	Bahamas Association of Compliance Officers Annual General Meeting	25 orgs.
May 05	Butterfield Bank (Bah.) Ltd.	16
June 17	Exuma rRadio “The Breeze 98.3”	04
June 18	Bahamas Association of Compliance Officers Anti-Money Laundering (AML) 1 day Seminar	60
Sept. 03	IBM (Bahamas) Ltd.	01
Nov. 17	St. Andrews School	17

December, 2008

TIP OF THE MONTH

This year on our website we promoted a monthly feature called “Tip of the Month” and were able to cover the following topics:-

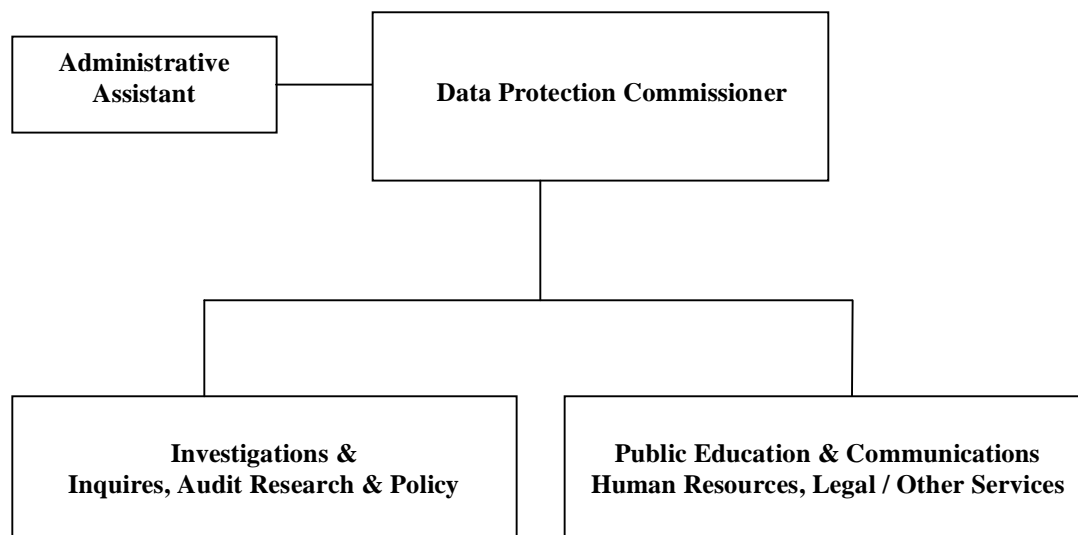
January	Exercise care with your personal information
February	“If it sounds too good to be true it’s probably not true!”
March	Do you have a Data Protection Problem?
April	The “Be my friend Craze” could get you in trouble!
May	Is it safe to have a “Cookie”?
June	Someone is “Phishing” for you and we’re not talking about the Nassau Grouper
July	Five (5) key principles of a sound security plan
August	Going on Vacation?
September	Protect your Medical Record
October	What are you doing with your old cell phone?
November	Do you really need my National Insurance Number?
December	Privacy Tips for Christmas Shopping

Brochures produced under the general theme of “Data Protection and You” are named below:-

- What you need to know and how it affects what you do!
- Identity Theft
- Why Complain?
- Are you ready for Data Protection?
- Managing a Data Security Breach
- Social Networking and Protecting our Children.

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 evolve 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 of 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 programmes 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 programmes 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 1st 2008 to 31st December, 2008

(Expressed in Bahamian Dollars)

Receipts

	2008	2007
Contribution provided via the Ministry of Finance (Note 1)	\$ 111,178	\$154,907
Total Receipts	\$111,178	\$154,907

Payments

Salary & Allowances (Note 2)	\$102,400	121,070
Travel & Subsistence	1,150	8,257
Training & Related costs	5,404	10,688
Office & Computer Equipment	360	6,020
Furniture & Fittings (Note 3)	-	7,408
Miscellaneous Expenditure	1,864	1,464
Total Payments	\$111,178	\$154,907

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**.
- Salaries & Allowances.**
 - The Commissioner is appointed by the Government initially for a term of three (3) years effective 26th October, 2006 and his remuneration and allowances are at rates determined by and agreed with the Minister of Finance. [Figure for 2007 (\$121,070) included a portion of year 2006].
 - 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 2008.

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, The Bahamas
Tel.: (242) 702-1553/ 702-1534
E-mail: dataprotection@bahamas.gov.bs
www.bahamas.gov.bs/dataprotection**