Data Protection (Privacy of Personal Information) Act, 2003

What you need to Know and How it affects what you do!
What is Data Protection?

- It is the safeguarding of the privacy rights of individuals in relation to the processing of personal information (data).
- The core element of data protection is that living individuals should be able to control how personal information about them is used, with or without their consent.
Introduction

As part of the e-Government initiative, 3 Acts were passed in April, 2003:-
2. The Data Protection (Privacy of Personal Information) Act. and,
3. The Electronic Communications and Transactions Act.
The focus here is on the Protection of Personal Information (Data).

Personal data means data relating to a living individual who can be identified either from the data or from data in conjunction with other information in the possession of the data controller.
Expectations

- We expect you to get an appreciation of the importance of this legislation and how it directly affects the way you deal with your clients going forward.
- You must have an open mind. It’s the law to protect personal information, having collected it fairly and; to ensure what you keep is accurate and up-to-date.
- The law expects you to provide personal information to relevant individuals upon request.
Main Purpose of the Act

• 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 data is used in a manner that is consistent with the intentions of the data subject.
Specific Topics of Review

- Brief Overview/Free Flow of Information
- Ombudsman
- Details of Personal Information
- Who is a Data Controller?
- Data Protection Principles
- Access to Personal Information
- Protecting against Identity Theft
- Duties of The Commissioner
- Powers of The Commissioner
- Transitional Provisions
Brief Overview

● The Data Protection (Privacy of Personal Information) Act, was passed into law in April 2003. It came into force on April 2, 2007.

● It sets 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), the OECD and the United Nations.
Free Flow of Information

- Free flow of personal data is vital to sustainable business within the global economy, particularly in:
  - the data services industry
  - the financial services industry
  - the airline industry
  - the hospitality industry and many others.
- These industries represent **BIG BUSINESS** for the Bahamas.
The Commissioner is a form of “ombudsman” – one who investigates reported complaints, reports findings, and helps to achieve equitable settlements.

He is a corporation sole and is independent in the performance of his duties.

He has responsibility for the administration and enforcement of the provisions of the Act.
Details of Personal Information

Personal Information may include:-

- Name, age, weight, height,
- Medical records,
- Income, purchases and spending habits,
- Race, ethic origin and color,
- Blood type, DNA code, fingerprints,
- Marital status and religion,
- Education,
- Home address and telephone number.

Your ability to control your personal information is key to your rights to privacy.
“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.
Who is a Data Controller?

- “Data Controller” 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.
- Under this Act the head of each government agency is a data controller and/or a “data processor” (one who processes personal information on behalf of the data controller).
8 Data Protection Principles

1. The data must be collected by means which are lawful and fair.
2. The data must be accurate and where necessary kept up to date (except in the case of back-up data).
3. The data shall be kept only for one or more specified and lawful purposes.
4. The data shall not be used or disclosed in any manner incompatible with that purpose or those purposes.
5. The data shall be adequate, relevant and not excessive in relation to that purpose or those purposes.

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.

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.
Data Principles Cont’d…

8. The data must not be transferred to another country unless that country has an adequate level of protection.
Access to Personal Information

Any individual making a written request to a data controller has a right, within 40 days, to:-

- Be informed by the data controller if the data kept on him include personal data relating to him.
- Be supplied with a copy of the information on him.
- Be entitled to an explanation to such information if appropriate. [Section 8 (1)].
Access to Personal Info. Cont’d

- It is advisable to fully acquaint yourselves with the full import of section 8 of the Act.
- Section 9 details several exceptions to section 8 including:
  - Information kept for law enforcement and personal security purposes; statistical and/or research purposes.
  - Information kept in the interest of national security and protecting international relations.
Protecting against Identity Theft
What is Identity Theft?

- Identity theft is the act of using someone’s personal information – such as account number, driver’s license, national insurance number, or employee identification badge – and using the assumed identity to commit fraud or theft.

- Today, it is one of the fastest growing crimes in North America!
Protecting against Identity Theft

- It is the responsibility of businesses to protect customer information and reduce the risk of identity theft.

- Personal information should be handled as if it were actual cash!

Steps for reducing the risk of identity theft:

1. Limit the amount of information collected.
2. Limit how long you retain the information collected.
3. Safeguard personal information against loss or theft.
Protecting against ID Theft Cont’d.

4. Safety at the check-out counter.
5. Discourage the use of NIB number as a “must see” form of identification.
6. Adopt good authentication processes.

If there is a data (security) breach:-
- Tell those affected.
- Let them know what you are doing and what they should do.
- Contact the police and other responsible agencies (Passport office, DPC, etc.).
- Take internal measures to contain the breach.
Duties of the Commissioner

- To promote the observance of good practice by data controllers within the Data Protection (POI) Act 2003 (“the DPA”).
- To provide information to the public on the legislation, how it works, and about other relevant matters.
- To issue codes of practice for guidance about data protection and to encourage similar codes by trade associations etc.
Duties Cont’d…

- To investigate any contravention of the DPA.
- To discharge, as the national supervisory authority, various functions relating to, or arising from any international obligations of the Bahamas in this regard.
Duties Cont’d…

- To execute other household duties as appropriate (staffing, accounts, etc.).
- To perform such 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 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:
   Power to issue prohibition notices, prohibiting the transfer of personal data in circumstances where data would lose its protection under the DPA.
Powers of the Commissioner Cont’d…

All notices are subject to appeal to the Supreme Court under section 24.

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).
Transitional Provisions

- Data Controllers have one year to have all necessary measures in place before an access request under section 8 becomes mandatory, \textit{i.e. until April 2, 2008.}\{Sect. 31. (1)\}.

- Section 31. (2) gives a five year grace period to continue using information now held, \textit{i.e. until April 2, 2012.}

- Thereafter, information held must be in compliance with the DPA 2003.

- \textbf{Start now and be ready!}
Data Security Plan!

According to the FTC, a sound data security plan is built on 5 key principles:

1. **Take stock.** Know what personal information you have in your files and on your computers.
2. **Scale down.** Keep only what you need for your business.
3. **Lock it.** Protect the information that you keep.
4. **Pitch it.** Properly dispose of what you no longer need.
5. **Plan ahead.** Create a plan to respond to security incidents.
Thank You!

Questions?

George E. Rodgers
Data Protection Commissioner
February, 2008
How to Contact Us

George E. Rodgers
Data Protection Commissioner
Second Floor
Cecil Wallace-Whitfield Centre
Cable Beach, West Bay Street
P.O. Box N-3017
Nassau, Bahamas
Telephone: 242-702-1552 Fax: 242-327-7501
Website: www.bahamas.gov.bs/dataprotection
Email: “dataprotection@bahamas.gov.bs”