
# A Guide for Data Controllers

**Data Protection (Privacy of Personal Information) Act, 2003**

# Data Protection Commissioner


## Acknowledgement

***Some of the information contained in this document has been extracted and/or modified from guidance documents published by other data protection jurisdictions around the world.***

**Definitions**

As with any legislation, certain terms have particular meaning. The following are some important definitions:

**Data** means information in a form which can be processed. It includes both equipment data and manual data.

**Back-up data** kept only for the purpose of replacing other data in the event of their being altered, lost, destroyed or damaged.

**Equipment data** means equipment for processing data.

**Manual data** means document or other material used in conjunction with, or produced by, data equipment.

**Personal data** means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller

**Processing** means performing any operation or set of operations on data, including:

- obtaining, recording or keeping the data
- collecting, organizing, storing, altering or adapting the data
- retrieving, consulting or using the data
- disclosing the data by transmitting, disseminating or otherwise making it available
- aligning, combining, blocking, erasing or destroying the data.

**Data Subject** is an individual who is the subject of personal data.

**Data Controller** is 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** is a person who processes personal information 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/her employment.

**Sensitive personal data** relates to specific categories of data which are defined as data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership.

***This booklet is intended as an introductory guide to those persons/agencies who are data controllers, in that they control the contents and use of personal data. It outlines the eight fundamental rules of data protection and presents them in a user friendly format. It is not an authoritative or definitive interpretation of the law, it is intended as a non-technical guide for data controllers. If, after reading this booklet, you require further information, please consult the Data Protection Commissioner's office at:***

***The Ministry of Finance***
***Cecil Wallace-Whitfield Centre***
***West Bay Street***
***P. O. Box N-3017***
***Nassau, Bahamas***
***Telephone: 242-701-1552***
***Fax: 242-327-7501***
***E-mail: dataprotection@bahamas.gov.bs***
***Website: www.bahamas.gov.bs/dataprotection***

**What is data protection?**
It is the safeguarding of the privacy rights of individuals in relation to the processing of personal data. The Data Protection (Privacy of Personal Information) Act 2003 ("the Act") confer rights on individuals as well as responsibilities on those persons processing personal data.

**Are you a data controller?**
If you, as an individual or an organization, collect, store and process any data about living people on any type of data equipment or in a structured filing system, (data material) then you are a data controller.

In practice, to establish whether or not you are a data controller, you should ask, do you decide what information is to be collected, stored, to what use it is put and when it should be deleted or altered? Because of the serious legal responsibilities attached to a data controller under the Act, you should seek the advice of the Commissioner if you have any doubts as to whether or not you are a data controller in any particular case.

**What are your responsibilities as a data controller?**
You have certain key responsibilities in relation to the information which you process. These may be summarized in terms of eight fundamental rules which you must follow. These rules which are detailed in this guide apply to all data controllers.

There are some specific requirements on which more detail can be found in the Act or by contacting this office directly. These include:

> The obligatory requirement to ensure that within one year after coming into force of this Act, Data Controllers must have the necessary measures in place that would allow the exercise of a request for access to personal data under Section 8 of the Act.
>
> Section 31 (2) gives a five year grace period to continue using personal information now held i.e. until April 2nd 2012. Thereafter, information held must be in full compliance with the Act.
>
> The right to prohibit processing for the purposes of direct marketing

**How do you as a data controller ensure compliance with the law?**
You must make yourself aware of your data protection responsibilities, in particular, to process personal data fairly. You should ensure that your staff are made aware of their responsibilities through appropriate training and/or the availability of an internal data protection policy. An internal policy which reflects the eight fundamental data protection rules, which is enforced through supervision and audit and reviewed regularly and is a valuable compliance tool.

**How is the Act enforced?**

The Commissioner's role is to ensure that those who keep personal information comply with the provisions of the Act. He has several enforcement powers to assist him in ensuring that the principles of data protection are being observed. These powers include the serving of enforcement Notices, and via Magistrate compelling data controllers to provide information needed to assist his enquires, or compelling a data controller to implement one or more provisions of the Act. He may investigate complaints made by the general public or carry out investigations proactively. He may, for example, authorize officers to enter premises and to inspect the type of personal information kept, how it is processed and the security measures in place. You and your staff must co-operate fully with such officers. A data controller found guilty of an offence on summary conviction, shall be liable to a fine not exceeding $2,000.00 (two thousand dollars).

A data controller found guilty of an offence under the Act shall be liable to a fine not exceeding $100,000.00 on conviction on indictment and/or may be ordered to delete all or part of the database.

# The Eight Rules of Data Protection

1. ***Personal 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 purposes.***

5. ***The data shall be adequate, relevant and not excessive in relation to that purpose or purposes.***

6. ***The data shall not be kept for longer than is necessary, (exceptions – historical, statistical or research purposes).***

7. ***The data shall be kept secure to avoid unauthorized or unlawful use, accidental loss or damage.***

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

## 1. Collect and process information fairly

To **fairly obtain** data the data subject must, at the time the personal data is being collected, be made aware of:

- the identity of the data controller
- the purpose in collecting the data, and
- the persons or categories of persons to whom the data may be disclosed
- any other information which is necessary so that processing may be fair.

To **fairly process** personal data it must have been fairly obtained, and:

- the data subject must have given consent to the processing or
- the processing must be necessary for one of the following reasons –
- to prevent injury or other damage to the health of a data subject
- to prevent serious loss or damage to property of the data subject
- to protect the vital interests of the data subject where the seeking of the consent of the data subject is likely to result in those interests being damaged
- for the administration of justice
- for the performance of a function conferred on a person by or under an enactment
- for the performance of a function of a Minister or the Minister of National Security
- for the performance of any other function of a public nature performed in the public interest by a person
- for the purpose of the legitimate interests pursued by a data controller except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject.

To **fairly process** sensitive data (see definitions) there are additional special conditions of which at least one of the following must be met:

- the data subject has given explicit consent to processing, i.e. the data subject has been clearly informed of the purpose/s in processing the data and has supplied his/her data with that understanding, or

- the processing must be necessary for one of the following reasons-

- for the purpose of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment

- to prevent injury or other damage to the health of the data subject or another person, or serious loss in respect of, or damage to, property or otherwise to protect the vital interests of the data subject or of another person in a case where, consent cannot be given, or the data controller cannot reasonably be expected to obtain such consent

- to prevent injury to, or damage to the health of, another person, or serious loss in respect of or damage to, the property of another person, in a case where such consent has been unreasonably withheld

- it is carried out by a not for profit organization in respect of its members or other persons in regular contact with the organization

- the information being processed has been made public as a result of steps deliberately taken by the data subject

- for the purpose of obtaining legal advice, or in connection with legal proceedings, or is necessary for the purposes of establishing, exercising or defending legal rights

- for medical purposes

- is carried out by political parties or candidates for election in the context of an election.

## 2. Keep it accurate, complete and up-to-date

To comply with this rule you should ensure that:

- your clerical and computer procedures are adequate to ensure high levels of data accuracy
- the general requirement to keep personal data up-to-date has been fully examined
- appropriate procedures are in place, including periodic review and audit, to ensure that each data item is kept up-to-date.

## 3. Keep it only for one or more specified, explicit and lawful purposes

You may only keep data for a purpose/s that are specific, lawful and clearly stated and the data should only be processed in a manner compatible with the purpose. An individual has a right to question the purpose for which you hold his/her data and you must be able to identify that purpose.

To comply with this rule:

- in general the persons whose data you collect should know the reason/s why you collect and keep it
- the purpose for which you collect and keep the data should be a lawful one
- you should be aware of the different sets of data which you keep and specific purpose of each.

## 4. Use and disclose it only in ways compatible with these purposes

Any use or disclosure must be necessary for the purpose/s or compatible with the purpose/s for which you collect and keep the data. You should ask whether the data subject would be surprised to learn that a particular use of or disclosure is taking place.

A key test of compatibility is:

- do you use the data only in ways consistent with the purpose/s for which they were obtained?

- do you disclose the data only in ways consistent with that purpose/s?

The rule, that disclosures of information must always be compatible with the purpose/s for which that information was obtained, is lifted in certain restricted cases by Section 13 of the Act. Examples of such cases would include some obvious situations where disclosure of the information is required by law or is made to the individual himself/herself or with his/her consent.

**5. Ensure that it is adequate, relevant and not excessive**

You can fulfill this requirement if you make sure you are keeping only the minimum amount of personal data which you need to keep to achieve your specified purpose/s. You should set down specific criteria to judge what is adequate, relevant, and not excessive and apply those criteria to each information item and the purpose/s for which it is held.

To comply with this rule you should ensure that the information held is:

- adequate in relation to the purpose/s for which you keep it
- relevant in relation to the purpose/s for which you keep it
- not excessive in relation to the purpose/s for which you keep it.

**6. Retain it for no longer than is necessary for the purpose or purposes. (Exceptions include data kept for historical, statistical, or research purposes)**

Nowadays information can be kept cheaply and effectively, particularly on computer. This requirement places a responsibility on data controllers to be clear about the length of time data will be kept and the reason why the information is being retained. You should assign specific responsibility for ensuring that files are regularly purged and that personal information is not retained any longer than necessary.

To comply with this rule you should have:

- a defined policy on retention periods for all items of personal data kept
- management, clerical and computer procedures in place to implement such a policy.

## 7. Keep it safe and secure

Appropriate security measures must be taken against unauthorized access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction. The security of personal information is all-important, but the key word here is appropriate, in that it is more significant in some situations than in others, depending on such matters as confidentiality and sensitivity and the harm that might result from an unauthorized disclosure. High standards of security are, nevertheless, essential for all personal information. The nature of security used may take into account what is available, the cost of implementation and the sensitivity of the data in question.

A minimum standard of security would include the following:

- access to the information restricted to authorized staff on a "need-to-know" basis in accordance with a defined policy
- computer systems should be password protected
- information on computer screens and manual files should be kept hidden from callers to your offices
- back-up procedure in operation for computer held data, including off-site back-up
- all reasonable measures should be taken to ensure that your staff are made aware of the organization's security measures, and comply with them
- all waste papers, printouts, etc. should be disposed of carefully
- a designated person should be responsible for security and there should be periodic reviews of the measures and practices in place
- premises should be secure when unoccupied
- a contract should be in place with any data processor which imposes equivalent security obligations on the data processor.

Apart from ensuring compliance with the Act, this requirement has an additional importance in that you may be liable to an individual for damages if you fail to observe the duty of care provision in the Act applying to the handling of personal data.

## 8. Give a copy of his/her personal data to that individual, on request

On making an access request any individual, about whom you keep personal data, is entitled to:

- a copy of the data you are keeping about him/her
- know your purpose/s for processing his/her data
- know the identity of those to whom you disclose the data
- know the source of the data, unless it is contrary to public interest
- know the logic involved in automated decisions
- a copy of any data held in the form of opinions, except where such opinions were given in confidence.

It is important that you have clear coordinated procedures in place to ensure that all relevant manual files and computers are checked for the data in respect of which the access request is being made.

To make an access request the **data subject must**:

- apply to you in writing
- give any details which might be needed to help you identify him/her and locate all the information you may keep about him/her e.g. previous addresses, customer account numbers
- pay you an access fee if you wish to charge one. You need not do so, but if you do it cannot exceed the prescribed amount. (To be advised by the Minister under Section 8 (3) of the Act).

Every individual about whom a data controller keeps personal information has a number of other rights under the Act, in addition to the Right of Access. These include the right to have any inaccurate information rectified or erased, to have personal data taken off a direct marketing or direct mailing list and the right to complain to the Data Protection Commissioner.

In response to an access request **you must**:

- supply the information to the individual promptly and within 40 days of receiving the request

- provide the information in a form which will be clear to the ordinary person, e.g. any codes must be explained.

If you do not keep any information about the individual making the request you should tell them so within the 40 days. You are not obliged to refund any fee you may have charged for dealing with the access request should you find you do not, in fact, keep any data. However, the fee must be refunded if you do not comply with the request, or if you have to rectify, supplement or erase the personal data concerned.

There are exceptions to the right of access in the interest of the data subject or the public interest. These are detailed in Section 9 of the Act.

**Transferring personal data abroad**

An area of concern for many data controllers are the requirements necessary for the transfer of data abroad. The Bahamas has to ensure that our data protection laws are consistent with internationally recognized principles established by the Council of Europe, The European Union (EU), The OECD and the United Nations. In addition, there are special conditions that have to be met before transferring personal data outside the European Economic Area, where the importing country does not have an EU approved level of data protection law. At least one of the following conditions must be met in that the transfer is:

- consented to by the data subject
- required or authorized under an enactment, convention or other instrument imposing an international obligation on this Country
- necessary for the performance of a contract between the data controller and the data subject
- necessary for the taking of steps at the request of the data subject with a view to his or her entering into a contract with the data controller
- necessary for the conclusion of a contract between the data controller and a third party, that is entered into at the request of the data subject and is in the interests of the data subject, or for the performance of such a contract
- necessary for the purpose of obtaining legal advice
- necessary to urgently prevent injury or damage to the health of a data subject
- part of the personal data held on a public register

- authorized by the Data Protection Commissioner, which is normally the approval of a contract which is based on the EU model.

And in all cases subject to the prevailing laws of The Commonwealth of The Bahamas.

As the legislation on the transfer of data abroad is complex, it may be advisable for persons to contact this Office in order to seek guidance on specific cases.

**Basic data protection checklist**

- Are the individuals whose data you collect aware of your identity?
- Have you told the data subject what use you make of his/her data?
- Are the disclosures you make of that data legitimate ones?
- Do you have appropriate security measures in place?
- Do you have appropriate procedures in place to ensure that each data item is kept up-to-date
- Do you have a defined policy on retention periods for all items of personal data?
- Do you have a data protection policy in place?
- Do you have procedures for handling access requests from individuals?
- Are you clear on whether or not you should be registered with the Office of the Data Protection Commissioner?
- Are your staff appropriately trained in data protection?
- Do you regularly review and audit the data which you hold and the manner in which they are processed?
- Do you have a copy of the Data Protection (POI) Act 2001 on hand for easy reference?