The Data Protection Ordinance 2004

What's it all about?

A guide for business, organisations & people

Government of Gibraltar
Ministry of Consumer & Civic Affairs
Ministry for Trade, Employment & Communication
Ministry for Financial Services

Coordinated by the Legislation Support Unit
No. 6 Convent Place

Contents

Data Protection – What's it all about?

As from January 2004 Gibraltar has had its own data protection law – the Data Protection Ordinance 2004.

The Ordinance is not currently in force, but will be commenced following a period of consultation.

This guide aims to inform readers in advance about the new law and what it will mean for people, businesses and public services in Gibraltar.

This guide is a general guide for information only and is not legal advice or a definitive statement of the law. To assist readers references are made to some of the relevant sections of the Ordinance.

The Data Protection Ordinance will affect all types of data held including information held by the police, and information held in computerised and manual forms.

Outline

We all have an interest in ensuring that personal data is accurate, kept up to date and used in a responsible and transparent way.

The main aim of the Data Protection Ordinance 2004 is to achieve just that. It helps both the holders of data and the people who are the subjects of the data, and strikes a balance between the rights of data subjects and the needs of businesses and service providers in Gibraltar.

The Data Protection Commissioner will have an important role in ensuring that the right balance is struck in Gibraltar. The Data Protection Commissioner will be the Gibraltar Regulatory Authority and will be independent of government.

What is 'Personal Data'?

The Ordinance is concerned with 'personal data'.

Personal data is information about people who can be identified. It can be any type of information – even something as simple as a name and address. The Ordinance does not apply to information kept about companies.

However the Ordinance does not cover the information kept for purely personal, household purposes such as personal address books and diaries.

Who are Data Subjects, Controllers and Processors?

Data subjects, data controllers, data processors and processing are key words used in the Ordinance.

A 'data subject' is a person about whom data is held; for example, if a bank keeps information about a Mrs. Gomez who is one of its clients, Mrs. Gomez will be the data subject.

All of us are data subjects. We are data subjects as employees – since our employer will keep information about us. We are data subjects as customers of banks or credit card companies since they will keep information about our accounts. We may be data subjects as students or parents of students since the school or college will keep information about us. We become data subjects every time we book a flight or holiday, when we apply for a job or even when we buy our groceries in the supermarket with a credit card.

A ‘data controller’ is the person who has or controls the use of the data. In the Mrs. Gomez example, the bank would be the data controller.

Sometimes data controllers send their data to an outside agency to be processed. For example, a large company may have their pay records processed by an outside company. In this case the outside agency would be called a ‘data processor’.

‘Processing’ of data is a very broad term: it includes the collecting, storing, making available and other use of data.

What are the Responsibilities of Data Controllers & Data Processors?

Data controllers and data processors will have responsibilities under the Ordinance whether they keep data in an automated, computerised form or in the form of manual, written records. In general, the same responsibilities in respect of manual and computer data.

Data Protection Principles

The primary responsibility of all data controllers is to abide by the Data Protection Principles. These principles are set out in section 6 of the Ordinance.

In simple terms the Data Protection Principles are as follows –

1. ***Fair & lawful obtaining & processing*** – the data must be obtained fairly and lawfully;

2. ***Accuracy*** – the data must be accurate and, where necessary, kept up to date;

3. ***Specific purposes*** – the data must be collected for a specific purpose or purposes and not further processed in a way incompatible with that purposes or those purposes; it must not be excessive in relation to that purpose or purposes and not kept for longer than necessary;

4. ***Security*** - appropriate security measures must be taken to prevent unauthorised access to, and accidental or unauthorised alterations to, data.

Data processors, as well as data controllers, must take the necessary security measures.

The costs of complying with these principles should not be large. Data controllers should also read the section of this guide on 'costs of complying' and 'conducting a data audit'.

Collecting Data Fairly and Lawfully

The Ordinance requires data controllers to let people know the purposes for which they intend to process data and to give them the information required by section 10.

Section 10 requires that -

- the data subject is informed of –
  - the identity of the data controller, and, if s/he has nominated a representative, the name of the representative,
  - the purpose or purposes for which the data are intended to be used,
  - any other relevant information which will enable the data subject to understand how the data will be used, such as - who will be given the information, whether replies to questions asked by the data controller are voluntary and the possible

consequences of not giving the information requested, the data subject's rights of access to and rectification of data;

- where the data controller has not collected the data directly from the data subject then s/he must also inform the data subject of –
  - the categories of data concerned, and
  - the name of the original data controller.

Use of Data only for specific purposes

The Ordinance prohibits the use of data for any purpose incompatible with the purpose for which it was collected and kept.

An easy way to understand what is an 'incompatible purpose' is to remember that the Ordinance aims for transparency in the use of data and data subjects must be told what the data is going to be used for (section 10). Thus, generally, a data controller should not use the data for a wholly different purpose without making sure that this is allowed by the Ordinance, for example by asking for the data subject's consent. The Ordinance allows the use of data for some purposes without obtaining the data subject's consent; for example to prevent damage to a person's health. For more information consult the Ordinance, the Data Protection Commissioner or obtain legal advice.

Security Measures

Data controllers and data processors must take appropriate organisational and security measures to ensure that data may not be -

- accessed by unauthorised persons or for unauthorised purposes,

- lost, altered, disclosed, or destroyed accidentally or unlawfully,
- otherwise unlawfully processed.

Most, or many, data controllers and data processors will already have security measures in place. Factors to consider include –

- ensuring personal data is not visible to the general public,
- locating computer terminals carefully so that casual visitors cannot read data from the computer screen,
- procedures to verify the identity of a person seeking information,
- storing manual records in a locked cabinet,
- use of computer passwords,
- staff training, staff manuals and disciplinary measures about appropriate security.

Data processors who disclose data without the prior authority of the data controller will commit an offence under the Ordinance punishable by a fine.

Keeping Data Confidential

In general it will be an offence to obtain or disclose personal data to a person other than a person authorised to receive it (section 12). For example, a person who 'hacks' into a company's staff or customer records kept on computer is likely to be guilty of an offence.

Direct Marketing

Direct marketing includes letters addressed personally to an individual promoting a product or service or telephone calls to an individual promoting a product or service (sometimes called 'cold calling'). Direct marketing includes situations where the data controller–

- itself uses names, addresses or other data to promote or sell its products or services, or
- provides names, addresses or other data to another body which uses the data to promote or sell products or services.

For example a garage holds the names and addresses of its customers, the garage owner (the data controller) gives those names and addresses to his brother who is setting up a camera shop. The brother writes out to all the customers promoting the new shop.

Direct marketing may be a nuisance and may even offend some people. Because of this the Ordinance introduces a right to object to the use of personal data for the purpose of direct marketing and data controllers must comply with data subjects' wishes. Where a data controller plans to use data for the purposes of direct marketing the data subjects must be informed of their right to object.

Use of data for the purposes of direct marketing may also be an incompatible use of data in breach of the data protection principles.

Legitimate use of data

Data may only be 'processed', i.e. collected, stored, given out or otherwise used, if the data protection principles are met, appropriate security measures are in place and one of the criteria in section 7 applies.

Those criteria include that –

- the data subject has given his or her unambiguous consent;
- the processing is necessary for a contract which the data subject wishes to enter into;

- the processing is necessary for health reasons or to prevent damage to property;
- the processing is necessary for the administration of justice or a public function.

The easiest way for data controllers to meet the section 7 criteria may be to ask the data subject for consent. For advice on the other criteria consult the Ordinance, the Data Protection Commissioner or obtain legal advice.

Sensitive Personal Data

Some types of data are known as 'sensitive personal data'. These are -

- data revealing racial or ethnic origin,
- data revealing political opinions,
- data revealing religious or philosophical beliefs,
- data revealing trade union membership,
- data concerning health or sex life,
- data concerning any criminal offence committed, or alleged to have been committed, by the data subject and the result of any criminal proceedings against him or her including any criminal sentence.

Because of the nature of the information, there are extra controls on the use of sensitive personal data. In addition to satisfying the data protection principles and the section 7 criteria data controllers who wish to process sensitive personal data must also make sure that they are complying with the criteria for processing sensitive personal data. Section 8(2) of the Ordinance sets out the circumstances in which sensitive personal data may be processed.

If you wish to process sensitive personal data, consult section 8(2) and, if necessary, consult the Data Protection Commissioner or obtain legal advice.

Transfer of Data outside Gibraltar

The Data Protection Ordinance controls the transfer of data from Gibraltar to other territories or countries. For the purposes of the Ordinance the UK is classified as a separate country.

Data may only be transferred out of Gibraltar to countries (or territories) –

- which are members of the European Economic Area[1], or
- which ensure an adequate level of protection for the privacy and fundamental rights and freedoms of data subjects.

Data controllers may also be able transfer personal data to other countries and territories if they are able to protect data subjects' rights, for example by means of contractual clauses.

The Data Protection Commissioner may prohibit the transfer of data from Gibraltar by issuing a 'Prohibition Notice'. It is an offence not to comply with a prohibition notice without reasonable excuse, but such notices may be appealed against.

If you require further information about transferring data outside Gibraltar please consult sections 30 and 31 of the Data Protection Ordinance 2004. The Data Protection Commissioner will also be able to help.

[1] From 1 May 2004 the countries of the European Economic Area will be – Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Holland, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, UK.

Use of data for the purposes of criminal investigations, tax collection, defence, etc.

The Data Protection Ordinance contains specific provisions related to these matters in sections 9 and 19. Persons concerned should contact the Data Protection Commissioner for further information.

The Data Processing Register

The Data Protection Commissioner will maintain a register of data processing operations conducted in Gibraltar.

The Register will be open for consultation by members of the public.

Do I have to register?

Most data controllers who keep data in computerised form will need to register their data processing operations with the Data Protection Commissioner.

Do remember - it is the processing operation which must be registered, not just the data controller. Even where a data controller has already registered various processing operations, if he begins a new type of processing operation that new processing operation must be registered as well – failure to do so will be a criminal offence.

In general data controllers will not need to register their processing operations if-

- they only process data manually,
- they only process data for the purpose of a register which is intended to provide information to the public and open to consultation.

Non-profit bodies such as clubs may be exempt from the requirement to register, but should consult the Data Protection Commissioner.

Some processing operations connected with defence, criminal investigations and certain other public functions may not need to be registered. Data controllers are advised to consult the Ordinance and the Data Protection Commissioner.

How do I register?

You should contact the Data Protection Commissioner for advice on how to register.

To register you will need to provide the following information –

- your name and address and the details of any representative;
- the types of data that you hold and the types of data subject – for example schools may hold data about students, their parents, and school employees;
- the reasons that you will process the data – for example, data on school employees will be held for purposes of employment, and pay records;
- the recipients or types of recipients to whom the data might be disclosed;
- any proposed transfer of data outside the European Economic Area;
- a description of the security measures taken with respect to data; and
- any other information reasonably required by the Data Protection Commissioner.

Data controllers have a duty to inform the Data Protection Commissioner of any changes to this information.

Even if you do not need to register with the data protection commissioner you must provide the information listed above directly to any person who requests it.

Rights of Data Subjects

Data subjects have a number of rights under the Data Protection Ordinance. They include rights –

- to have data about themselves collected, stored and used in a manner compatible with the data protection principles;
- to access data about themselves;
- to have incorrect data about themselves corrected;
- to object to the use of data for the purposes of direct marketing;
- not to have decisions made about them solely on the basis of automatic processing of data; and
- to complain to the Data Protection Commissioner and to take legal action against the improper use of personal data.

The Data Protection Principles

See above under the responsibilities of data controllers and data processors.

Right of Access

There are two slightly different rights of access to data:-

1. A right to general information

Data subjects have a right to make a written request to any person or company which they believe keeps personal data and, within 21 days of that request, the person or company must inform them in writing, in general terms, whether they do keep any data, and if so what type of data they keep. In essence this is

the same sort of information that the data controller will provide to the Commissioner when they register. Some companies may find it useful to provide this type of information in the form of a pre-prepared information sheet. No fee may be charged for supplying this type of information. (section 14(1)).

2. A right to information concerning themselves
Data subjects have a right of access to information concerning themselves. If a data subject makes a written request to a person, company or public body which they believe processes information about them, that person, company or public body must respond in writing within 28 days providing the information set out in section 14(3) of the Ordinance. A fee may be charged for providing such information, but any fee must be refunded if the request is not complied with within the specified time or the information held by the data controller is found to be incorrect and is amended (section 14(6)).

In some limited situations the right of access of data subjects to data about themselves will not apply, for example in respect of criminal investigations (section 19).

Generally data controllers are not required to provide personal data relating to any person other than the person making the request. However there are exceptions – see sections 14(9), 14(10) of the Ordinance. Section 14(15) contains specific provisions about employment references.

If you require further information about access rights you should consult the Ordinance, the Data Protection Commissioner or take legal advice.

Right of Rectification

The Data Protection Principles require that data held under the Data Protection Ordinance must be accurate.

Data subjects have the right to require data controllers to rectify or destroy inaccurate data about them and data controllers must comply with the request within 28 days (section 15).

Right to object

Data subjects have a right to object to the use of data in a number of situations.

They have -

- a right to object to the use of data for purposes of direct marketing (section 17); and
- a right to object to the processing of data in some circumstances where the processing will cause 'substantial damage or distress' to the data subject or to another person (section 16).

Right not to have decisions made solely on the basis of automated data

Decisions concerning a data subject generally must not be made solely on the basis of automated data if the decision will have a legal or other significant effect on the data subject (section 18). For example, decisions as to examination results or whether or not to grant a mortgage or loan. There is an exception to this rule if –

- the data subject consents, or
- one of the exceptions in section 18(2)(b) applies.

What to do if your rights are violated?

If you think your rights may have been or are being violated contact the Data Protection Commissioner for help.

The Data Protection Commissioner has powers to resolve problems relating to data protection and can order that financial compensation be paid to a data subject.

If you are not happy with the results of your complaint to the Data Protection Commissioner you may be able to appeal to the courts.

The Role of the Data Protection Commissioner

The Data Protection Commissioner has the following functions -

- ensuring good practice in data protection in Gibraltar;
- providing information and assistance, education on data protection;
- acting as guardian of the Data Protection Ordinance;
- mediating in disputes about personal data and awarding compensation for damage suffered by data subjects; and
- keeping the Data Protection Register.

To ensure good practice in data protection the Data Protection Commissioner may draw up codes of practice in consultation with relevant parties.

Any data subject who has a complaint about data protection may contact the Data Protection Commissioner for help. The Data Protection Commissioner may be able to help the parties resolve disagreements about data protection issues. He also has the power to award compensation to data subjects if they have suffered damage as a result of a breach of the Ordinance.

The Data Commissioner can also –

- require persons to provide him with information (by issuing an 'information notice'),
- require steps to be taken (by issuing an 'enforcement notice'), or
- prohibit the transfer of personal data outside the European Economic Area (by issuing a 'prohibition notice').

It will be an offence to fail to comply with these notices without reasonable excuse, to supply false or misleading information or to obstruct 'authorised officers' of the Data Protection Commissioner.

The Data Commissioner will have powers to enter and search premises and seize property to assist him with his work.

Decisions of the Commissioner may be challenged in the courts.

Where to go for help and Information

The Data Protection Commissioner can provide further information and assistance regarding data protection.

Data Protection Commissioner,
C/o Gibraltar Regulatory Authority,
Suite 811 Europort, Gibraltar.
Tel: 74636 Fax: 72166
Email: info@gra.gi

Anyone wishing to find out more about data protection may find the following websites helpful. But, please do remember that it is the Gibraltar legislation which must be complied with in Gibraltar.

- Irish Data Protection Commissioner – http://www.dataprivacy.ie/docs/Home/4.htm
- UK Data Protection Commissioner – http://www.informationcommissioner.gov.uk/
- European Commission – http://europa.eu.int/comm/justice_home/fsj/privacy

You can obtain a copy of the Data Protection Ordinance at –

http://www.gibraltarlaws.gov.gi

Costs of Complying with Data Protection Ordinance

Businesses and services may incur some costs in complying with the Data Protection Ordinance. Every effort has been made to keep these as low as possible.

The cost of compliance may vary considerably from business to business and will depend in large part on the current practices – some companies and organisations will find that they are already complying with the data protection principles; others will find that they need to take steps to change their current practices.

A major cost for business be in conducting an initial 'data audit' of the requirements set out in the Ordinance.

The attached checklist from the Irish Data Protection Commissioner may be helpful in conducting a 'data audit', but please do remember that you will need to make sure that you comply with the Gibraltar legislation, rather than the Irish.

The cost of complying with the Data Protection Ordinance will depend largely on the current practices of your business. They may include -

General Costs of Compliance

- Preparing for compliance — Costs of conducting audit of current business practices, introducing changes and training staff.

- Failure to comply — Data controllers who do not comply with the Ordinance may be subjected to criminal fines and, or, obliged to pay compensation. There may be legal costs.

  However data controllers may currently

	be liable in negligence where they make decisions on the basis of incorrect data.

Ensuring personal data is held in conformity with the data protection principles:

• Fair & lawful obtaining	Costs of providing data subjects with the information required by section 10. Businesses may choose to do this by producing an information sheet available to data subjects.
• Data is to be accurate	There may be a cost in reviewing existing data and ensuring that new data obtained is accurate.
• Use for specified, explicit and legitimate purposes, not excessive and not kept for longer than necessary for those purposes.	There may be a cost in reviewing existing data and existing businesses practices to ensure compliance. Data subjects will need to be informed that data about them will be held and processed and for what purposes.
• Security Measures	Cost of reviewing technical and organisational data security. Costs could include training staff on data security or purchasing equipment.

Ensuring data is processed in accordance with the Ordinance:

• Data processed in compliance with section 7	Cost of reviewing business practices and, if necessary, introducing new practices.
• Sensitive data processed in compliance with section 8	Cost of reviewing business practices and, if necessary, introducing new practices.

Confidentiality

• Ensuring that confidentiality requirements are complied with	Not possible to cost.

Data Subjects' Rights:

• Access	Cost of providing general information about data protection, businesses may wish to make available an information sheet. Costs of supplying information on data held about individuals who request it, but this may be recouped by charging a fee. No fee may be charged where the data held by the Data Controller is inaccurate.
• Rectification, erasure or blocking of incorrect personal data	Cost of informing data subjects in writing that rectification etc. of data has taken place, but the Data Controller has a general duty to ensure that personal data is accurate.
• Data Subjects' rights to object	Not possible to cost, potential costs can be avoided by requesting the consent of the data subject to the processing. Cost of responding in writing with written requests of data subjects.
• Direct marketing	Cost of informing data subjects' of their right to object to direct marketing. Cost of responding to data subjects' requests not to have data used for direct marketing.
• No decisions solely on automatic processing	Not possible to cost; businesses which wish to rely solely on automatic processing may need to ensure that their processes comply with section 18.

Registration with the Data Commissioner	
• Registration	One off cost of registering processing operations. Some businesses and, or, processing operations will be exempt.
Prohibitions on Transfer of Data	Not possible to cost. Possible legal costs for some businesses who transfer data outside of the EEA.

Conducting a Data Audit for Data Controllers

Data Protection Checklist[2]

Assess your own Data Protection Policy

Having learned about the legal responsibilities you have as a data controller under the Data Protection Ordinance, it will be clear that these responsibilities will not be met unless the issues involved are specifically examined in a structured manner and the results of that examination converted into a clear policy position on data protection.

This self-help questionnaire is designed to help you in carrying out such an exercise, and may assist you to formulate a policy statement on data protection. The level of detail which you find useful will obviously depend on the amount and type of personal data which you keep, but you should review all issues mentioned. Please note, this check-list does not cover all of your responsibilities under the Data Protection Ordinance and you will need to check the Ordinance as well to ensure that you are complying with it correctly.

Self-help checklist on data protection policy

If you can answer YES to all the questions below, your business is in good shape from a data protection viewpoint. If not, the checklist can help you identify the areas where you need to improve in order to comply with the Data Protection Ordinance.

---

[2] *This check-list has been adapted for use in Gibraltar from the check-list written by the Irish Data Protection Commissioner.*

Main responsibilities

Fair obtaining:

- ❑ At the time when we collect information about individuals, are they made aware of the uses for that information?
- ❑ Are people made aware of any disclosures of their personal information to third parties?
- ❑ Have we obtained people's consent for any secondary uses of their personal information, which might not be obvious to them?
- ❑ Can we describe our data-collection practices as open, transparent and up-front?

Purpose specification

- ❑ Are we clear about the purpose (or purposes) for which we keep personal information?
- ❑ Are the individuals about who we keep personal information also clear about this purpose (or purposes)?
- ❑ If we are required to register with the Data Protection Commissioner, does our register entry (or entries) include a proper, comprehensive statement of our purpose (or purposes)? [Remember, if you are using personal information for a purpose not listed on your register entry, you may be committing an offence.]

- ❑ Has responsibility been assigned to a member of staff for maintaining a list of the different types of personal information which we keep and the purpose associated with each different type?

Use and disclosure of information

- ❑ Do we have clear defined rules about the use and disclosure of personal information?

- ❑ Do those rules comply with the Data Protection Ordinance?

- ❑ Are all staff aware of these rules?

- ❑ Are the individuals about whom we keep personal information aware of the uses and disclosures of their personal information? Would they be surprised if they learned about them? Consider whether the consent of the individuals should be obtained for these uses and disclosures.

- ❑ If we are required to register with the Data Protection Commissioner, does our register entry (or entries) include a full list of persons to whom we may need to disclose personal information? [Remember, if you disclose personal information to someone not listed on your register entry, you may be committing an offence.]

Security

- ❑ Do we have a list of security provisions in place for each different type of personal information including both information kept on computer and

data kept in manual records (i.e. non computerised)?

- ❑ Do we have a procedure for the development and review of these security provisions? Is someone responsible for this?

- ❑ Are these security provisions appropriate to the sensitivity of the personal information which we keep?

- ❑ Are our computers and our databases password-protected, and encrypted if appropriate?

- ❑ Are our computers and our servers securely locked away from unauthorised people?

- ❑ How do we store personal information which is in manual form (ie not on a computer)? Is this information securely kept from unauthorized people?

Adequate, relevant and not excessive

- ❑ Do we collect all the personal information we need to serve our purpose(s) effectively, and in a way which treats individuals in a fair and comprehensive manner?

- ❑ Have we checked to make sure that all the personal information we collect is relevant, and not excessive, for our specified purpose(s)?

- ❑ If an individual asked us to justify every piece of information we hold about him or her, could we do so?

- ❑ Do we have a policy in this regard?

Accurate and up-to-date

- ❑ Do we check that the personal information we hold about individuals is accurate?

- ❑ Do we know how much of the personal information we hold about individuals is time-sensitive, i.e. likely to become inaccurate over time unless it is updated?

- ❑ Do we take steps to ensure that the personal information we hold about individuals is kept up-to-date?

Retention time

- ❑ Do we have a clear policy on how long we keep items of personal information about individuals?

- ❑ Are we clear about any legal requirements on us to retain personal information for a particular period of time?

- ❑ Do we regularly purge our manual and computer records of personal information which we no longer need, such as personal information relating to former customers or former staff members?

- ❑ Do we have a policy on deleting personal information as soon as the purpose for which we obtained the data has been completed?

The Right of Access to Personal Information

- ❑ Is a named individual responsible for handling requests for access to personal information?
- ❑ Are there clear procedures in place for dealing with such requests?
- ❑ Do these procedures guarantee compliance with the requirements of the Data Protection Ordinance?

Registration

- ❑ Are we clear about whether or not we need to register with the Data Protection Commissioner?
- ❑ If registration is required, is the registration kept up to date? Does the registration accurately reflect our practices for handling personal information? Does the registration accurately reflect all of our processing operations? [Remember, if your data-handling practices are out of line with the details set out in your register entry(ies), you may be committing an offence.]
- ❑ Is a named individual responsible for meeting our registration requirements and ensuring that our registration is kept up to date?

Training & Education

- ❑ Do we know about the levels of awareness of data protection in our organisation?

- ❑ Are all of our staff aware of their data protection responsibilities - including the need for confidentiality?

- ❑ Is data protection included as part of the training programme for our staff?

Co-ordination and Compliance

- ❑ Have we appointed a data protection co-coordinator and compliance person?

- ❑ Are all staff aware of his or her role?

- ❑ Are there mechanisms in place for formal review by the co-coordinator of data protection activities within our organisation?

- ❑ Are we required by the Data Protection Ordinance to appoint a personal data protection official? If so have we appointed one and ensured that they are equipped to undertake their role?

Additional copies of this guide may be obtained at
www.gibraltar.gov.gi