

Introduction

With the ever increasing use of computers in our daily lives and their ability to store and process data, the protection and safeguarding of personal data is becoming increasingly important in today's world.

Most if not all businesses keep some record of their individual customers, and with the ever increasing use of the internet to conduct on-line transactions, more and more of us are parting with personal information, leaving us exposed to the potential misuse of this information by others.

The Data Protection Act 2004

Last summer the Data Protection Act 2004 came into force in Gibraltar. The Act was designed to provide rights and freedoms to individuals against businesses and other organisations processing personal data. It also imposed certain responsibilities and obligations on the processors of such data. This article will highlight some of the issues businesses need to be aware of following the introduction of the Act, and serves as a reminder for the need for an effective data protection policy to be formed.

In addition it must be noted that the Act applies to all storage and retention of data, even if it is written down and kept in a filing cabinet; it is not just information stored on a computer.

The exception to all this is when data is processed purely for personal reasons. Then, in such circumstances the provisions of the Act do not apply.

Principles

However, if your business keeps or processes any information about living people it will need to comply with the eight basic principles of data protection:

1. Obtain and process the information fairly
2. Keep it only for one or more specified and lawful purposes
3. Process it only in ways compatible with the purposes for which it was given to you initially – for example if you say it is to keep your customers up to date with new product information, you cannot then sell their details on to a telemarketer
4. Keep it safe and secure – for example, your staff need to be told that that they must keep personal information securely and in accordance with any security procedures you have established.
5. Keep it accurate and up-to-date
6. Ensure that it is adequate, relevant and not excessive
7. Retain it no longer than is necessary for the specified purpose or purposes
8. Give a copy of his/her personal data to an individual, on request

In addition to these basic principles, if you are processing sensitive personal information an additional obligation of obtaining the individual's explicit consent is imposed.

Sensitive data can be classified as any information relating to a person's racial or ethnic origin, religious or philosophical belief, trade-union membership, health records or sex life. It also includes the commission or alleged commission of any offence, as well as information relating to any proceedings and any sentence handed out.

Although there are exceptions to the requirement to obtain consent, these are usually limited to situations when it is either not possible to obtain consent for say, practical reasons, or when the processing of this information is done for the purposes of the protection of the vital interests of the individual or for some other public purpose.

Staff

In addition to the principles outlined above, the Act imposes a requirement for businesses to take reasonable steps to ensure that employees and other people who attend the workplace are aware of and comply with the relevant data security measures in place. Of particular importance are those security measures put in place to protect against the accidental or unlawful destruction or the unauthorised access or disclosure of personal information. This can be achieved by regular updates to staff together with training as and when the need arises.

Registration

It should be noted that under the Act, it is an offence for businesses to process personal data unless they have first registered their data processing operations with the Data Protection Commissioner. Registration is done by written application to the Commissioner and it must contain certain information which is set out in the Act.

Rights

It is also equally important for businesses to know what the various rights are of the individuals whose data they are processing and how to deal with requests from people asserting these rights.

The basic rights include, among others, the rights for individuals to have access to the information your business holds about them. If the information is inaccurate, you can be required to correct this. In addition individuals have the right to object to decisions being made about them as a result of the automated processing of their information. Breaches of these rights can lead to a complaint being made to the Data Protection Commissioner and can result in legal action being taken against the business.

Data Person

In light of the above, it is well worth appointing a specific person in the business to deal with all things relating to data protection. This person should be responsible for processing individual data access requests and dealing with specific objections to the use of personal data.

Such requests need to be dealt with properly within 21 days and failing to do this within this time limit is an offence under the Act. Furthermore it leaves the business open to the individual concerned to complain to the Data Protection Commissioner. Complaints of this nature can lead to an order being made for financial compensation to be paid to the complainant and businesses should not underestimate also other effects of non compliance, which could include loss of consumer trust and loyalty.

Ecommerce

If your business operates a website or uses forms requiring consumers to part with personal information, a Privacy Statement must be prepared. The Privacy Statement must be attached to the forms and must appear also on the website. It should make clear in plain language, and with appropriate prominence, precisely what is being consented to. A more in depth analysis of the contents of Privacy Statements will be the subject of a future article.

Checklist

There is a useful checklist put together by the Government of Gibraltar to help businesses and other organisations establish if they are compliant with the various requirements of the Act. It is well worth going through this checklist to see whether your business has an effective data protection policy. The checklist can be accessed on-line by entering the following GRA link: http://www.gra.gi/Data_Protection/docs/Simple_guide.pdf.

In addition Hassans is able to assist your business with the preparation of effective data protection policies as well as training staff as to their obligations under the Act.

For further information please contact Stephen Forster or Michael Nahon.

Stephen.forster@hassans.gi

Michael.nahon@hassans.gi