Data Controllers
Overview of Data Protection Law

The Data Protection Law provides a framework for the processing of data relating to individuals that serves to balance the needs of organisations to conduct legitimate business against the rights of individuals to see that their information is securely and appropriately handled.

This guidance note provides an overview of the Law from the organisation's perspective, including their obligations and an outline of the rights of individuals.

This guidance relates to both the Data Protection (Jersey) Law 2005 and the Data Protection (Bailiwick of Guernsey) Law, 2001.

Where the Laws differ and to show differences between the two jurisdictions the page will be split as shown below.

Jersey	Guernsey
Commissioner = Information Commissioner a = article within the Law	Commissioner = Data Protection Commissioner s = section of the Law

Where numbering of passages from the Laws are the same it will be shown as a/s.

Table of Contents

Introduction

The growth in the use of personal data has many benefits, both for society, like helping to fight crime and for the individual, like better medical care. However, whenever personal data are collected and used, people's lives can be adversely affected if something goes wrong.

For example, if details are not entered correctly individuals can be unjustly refused credit, benefits, housing, or even a job. If data are not kept securely, an individual's privacy can be affected. It is vital that those who collect and use personal data maintain the confidence of those who are asked to provide it by complying with the requirements of the Data Protection Law ("the Law").

The Law applies to "personal data" that is, data about identifiable, living individuals. Those who decide how and why personal data are processed, must comply with the rules of good information handling, known as the Data Protection Principles, and the other requirements of the Law.

Definitions

Personal data - is information that relates to and identifies *living* individuals, i.e. their personal information. Personal data includes both facts and opinions about the individual, as well as information regarding the intentions of the data controller towards the individual.

Data subjects - are the living individuals to whom the personal data relate.

Processing – covers a wide range of operations on personal information, this includes its collection, use, disclosure and disposal.

Data controllers - are those who determine the purpose(s) for which and the manner in which personal data are processed. This can be any type of company or organisation, large or small, within the public or private sector. A data controller can also be a sole trader, partnership, or an individual.

Data processors – are those who are not employed by a data controller but who process personal data on behalf and in accordance with the

instructions of a data controller; in effect they could be referred to as subcontractors. For example where a data controller outsources its payroll function, the organisation that handles that on the data controller's behalf would be a data processor.

What does the Law cover?

The Law covers information that is processed electronically, information that is processed in hard copy form with an intention to process it electronically and manual records held in a "relevant filing system".

A relevant filing system is a set of information in which the records are structured, either by reference to individuals or by reference to criteria relating to individuals, so that "specific information relating to a particular individual is readily accessible". The definition means a significant amount of manual data falls under the scope of the Law, particularly in the field of staff administration.

The rules of good information handling – the principles

Anyone processing personal information must comply with the eight enforceable principles of good information handling. These say that personal information must be:

1. fairly and lawfully processed;
2. processed for limited purposes and not in any manner incompatible with those purposes;
3. adequate, relevant and not excessive;
4. accurate and, where necessary, kept up to date;
5. not kept for longer than is necessary;
6. processed in line with the individual's rights;
7. kept secure; and
8. not transferred to countries outside the Bailiwick and European Economic Area (EEA) that do not have adequate data protection

First Principle – fair processing

In general terms, the First Principle requires that information should be "fairly processed", i.e. when you collect the information from individuals you should be honest and open about why you want it. In addition you must have a legitimate reason for processing the data. You should explain (in most cases in writing):

- Who you (the data controller) are – giving the name of your organisation;
- What you intend to use the information for;
- To whom you intend to give the personal data. This may be a specific third party, or may be a more general description such as "other relevant services".

First Principle – lawful processing

The second half of the First Principle relates to processing needing to be lawful. Processing may be deemed to be lawful where one of the following conditions has been met (found in Schedule 2 of the Law):

- the individual has given his or her consent to the processing;
- the processing is necessary for the performance of a contract with the individual;
- the processing is required under a legal obligation;
- the processing is necessary to protect the vital interests of the individual;
- the processing is necessary to carry out public functions;
- the processing is necessary in order to pursue the legitimate interests of the data controller or third parties (unless it could prejudice the interests of the individual).

Processing sensitive personal data

The Law makes specific provision for sensitive personal data. Sensitive personal data include: racial or ethnic origin; political opinions; religious or other beliefs; trade union membership; health; sex life; criminal proceedings or convictions.

Sensitive personal data can only be processed under strict conditions, which include;

- having the explicit consent of the individual;
- being required by law to process the data for employment purposes;
- needing to process the information in order to protect the vital interests of the data subjects or another;
- the administration of justice or legal proceedings.

A full list of conditions for the lawful processing of sensitive personal data can be found in Schedule 3 of the Law.

Second Principle - specified and lawful purposes

The Second Principle requires that personal data will be used only for the aims and purposes that the organisation has specified and for which it has been established. In the event that the data might be processed for other purposes then consent would have to be obtained for this additional use.

Third Principle - adequate, relevant and not excessive

The Third Principle requires you to hold only the data which you actually need.

Data controllers should monitor the quantities of information held for their organisation's purposes and ensure that they hold neither too much nor too little in respect of their clients. For instance, many organisations routinely collect clients' dates of birth. In some cases this may be

relevant, for instance if they are considering providing services for those in a certain age group. But in other situations, this data may be excessive. For example for your purposes all you may actually need to know is whether your clients are over sixty-five years old.

Fourth Principle - accurate

The Fourth Principle requires that personal data should be accurate. This makes sense as the result of processing inaccurate data normally leads to services being ineffective and inefficient. Users of services can experience negative outcomes, both tangible and intangible, due to inaccurate processing of their personal data.

Fifth Principle - no longer than necessary

It is only in exceptional circumstances that personal data should be kept indefinitely. In order to comply with the Fifth Principle you should have a procedure for the removal of different categories of data from your system after certain periods, for instance, when the information is no longer required for audit purposes or when a client no longer requires your services.

Sixth Principle – rights of individuals

The right of subject access

The Law allows individuals to find out what information is held about themselves on computer and some paper records. This is known as the right of subject access.

Organisations can charge a £10 fee for complying with a subject access request and request any identification necessary to assure themselves of the identity of the applicant.

Subject access requests are covered in more detail in the specific subject access guidance note, located on our website.

The right of rectification, blocking, erasure and destruction

The Law allows individuals to apply to the Court to order a data controller to rectify, block, erase or destroy personal details if they are inaccurate or contain expressions of opinion which are based on inaccurate data.

The right to prevent processing

An individual can ask a data controller to stop or request that they do not begin processing relating to him or her where it is causing, or is likely to cause, substantial unwarranted damage or substantial distress to them or anyone else. However, this right is not available in all cases and data controllers do not always have to comply with the request.

The right to prevent processing for direct marketing

An individual can ask a data controller to stop or not to begin processing data relating to him or her for direct marketing purposes. This is an absolute right; data controllers must not send direct marketing material to anyone who has asked not to receive it.

The right to compensation

An individual can claim compensation from a data controller for damage or damage and distress caused by any breach of the Law.

Jersey	Guernsey
Compensation can also be claimed for distress.	Compensation for distress alone can only be claimed in limited circumstances.

Rights in relation to automated decision-taking

An individual can ask a data controller to ensure that no decision which significantly affects them is based solely on processing his or her personal data by automatic means. There are, however, some exemptions to this.

Seventh Principle - security

Data controllers must take security measures to safeguard personal data. The Law requires that data controllers to take appropriate technical or organisational measures to prevent the unauthorised or unlawful processing, or disclosure, of personal data.

Where a controller uses the services of a data processor the security arrangements must be part of a written agreement between the two parties. A processor is an external agency to whom the controller may outsource certain activities such as payroll.

Eight Principle - transfer of personal data overseas

The Eighth Principle restricts the transfer of personal data outside the EEA (which consists of the EU Member States, Norway, Iceland and Liechtenstein). Personal data may only be transferred to third countries if those countries ensure an "adequate level of protection for the rights and freedoms of data subjects".

More information can be found in the dedicated International Transfer guidance note, located on our website.

Notification

Most data controllers will need to notify the Commissioner, in broad terms, of the purposes of their processing, the personal data processed, the recipients of the personal data processed and where the data may be transferred. This information is made publicly available in a register. Notification is not linked to enforcement. Under the Law all data

controllers must comply with the Data Protection Principles, even if they are exempt from the requirement to notify. Notifications are renewable annually.

The Notification register may be viewed online at www.dataci.org. This site also includes an online notification service and self-assessment questions on exemption.

Criminal Offences

Notification offences

These are committed where processing is being undertaken by a data controller who has not notified the Commissioner either of the processing being undertaken or of any changes that have been made to that processing. Failure to notify is a strict liability offence.

Procuring and selling offences

It is an offence to obtain, disclose, sell or advertise for sale, or bring about the disclosure of personal data, without the consent of the data controller. It is also an offence to access personal data or to disclose it without proper authorisation. This covers unauthorised access to and disclosure of personal data. There are some exceptions to this.

Other offences

It is an offence to fail to respond to an information notice or to breach an enforcement notice issued by the Commissioner. Unauthorised disclosures by the Commissioner or her staff are forbidden and a breach of those provisions is an offence.

Contact the Commissioner

Enquiries and Publication Requests

Jersey

Office of the Information Commissioner
Brunel House
Old Street
St Helier
Jersey
JE2 3RG

T: +44 (0)1534 716530
W: www.dataci.org
Email: enquiries@dataci.org

Guernsey

Office of the Data Protection Commissioner
Guernsey Information Centre
North Esplanade
St Peter Port
Guernsey
GY1 2LQ

T: +44 (0)1481 742074
W: www.dataci.org
Email: enquiries@dataci.org