THE OFFICE OF THE
DATA PROTECTION
COMMISSIONER

General Advice & Guidance for States Members

Data Protection (Bailiwick of Guernsey) Law, 2001

Table of Contents

May 2016

Introduction

The Data Protection (Bailiwick of Guernsey) Law, 2001 ('the Law') regulates the processing of information relating to living individuals, including the obtaining, holding, use or disclosure of such information, and the purposes for which that information is used or held in connection with. The type of information covered by the Law can be as little as a name and address. The Law gives enforceable rights to individuals (data subjects) and places obligations on those persons who control the manner and the purpose of the processing of personal data (data controllers).

Anyone processing personal information (with limited exemptions) must notify the Data Protection Commissioner ('the Commissioner') as a data controller and provide details of their processing. These details are published by the Commissioner on an on-line public register.

This document aims to assist States Members in achieving compliance with the Law and accompanying Regulations. Should you have any queries regarding notification, interpretation or application of the Law, please contact the Commissioner, who will be glad to assist. Alternatively, please visit our website for further information.

Is there a need to Notify?

Acting on behalf of a Committee?

In considering whether there is a requirement to notify, Members must decide in which capacity they intend to process personal data.

States Members who sit on a Committee, or work directly with a service area (eg as a President) are likely to have access to and process personal data held at departmental level in the same way as civil service employees. In such a situation, the data controller is the service area rather than the member. The service area is, therefore, legally responsible for the information and potentially liable for any breach. An example is the Committee *for* Home Affairs who decide upon the issuance of compassionate housing licences and process personal data as a result.

Acting on own behalf?

If Members process personal data to act on their own behalf, they are likely to have to notify in their own right. Examples include the processing of personal data in order to timetable surgery appointments or progress complaints or enquiries made by local residents.

Any Member who is unsure of whether or not they need to notify should contact the Office of the Data Protection Commissioner for further advice.

Any individual or organisation processing personal data must comply with the Law and the Eight Data Protection Principles as detailed below.

The 8 Data Protection Principles

Data controllers must comply with eight data protection principles, which together form an enforceable framework for the proper handling of personal data.

First Principle:
Processing is fair and lawful

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

(a) at least one of the conditions in Schedule 2 is met (see Appendix 1); and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met (see Appendix 2).

What this means:

Basically this means there are certain conditions for the processing of any personal data. At least one of these conditions must be satisfied before any processing can commence.

Firstly, is there a law which requires the processing? This is likely to be the case for many States entities. Any processing must then be done in accordance with those statutory powers.

Secondly has the collection and use of personal data been fair? Essentially this requires the data controller to ensure that those individuals whose data are being processing have not been deceived or misled as to the purpose for which their information is being processed.

Thirdly it is important to establish compliance with one of the relevant conditions in Schedules 2 or 3 (depending on whether it is personal data or sensitive personal data that is being processed). Please refer to Appendices 1 and 2 for details of the conditions.

Case Study 1:

The Electoral Roll is prepared by the Registrar-General of Electors. It contains personal data relating to those Bailiwick residents who are eligible to vote and must only be used for election purposes.

There is a requirements within the accompanying legislation that the Electoral Role be made available for inspection at Sir Charles Frossard House and the Guille-Alles Library. Copies of the relevant section of the register can also be given to persons standing for election once the nominations have been made.

It is therefore not permitted for a States Member to either inspect the data, or obtain copies of the data for purposes other than public elections, for example, to establish the address of a constituent in relation to a dispute between two parties. To do so would constitute unfair processing and would breach the first principle.

Second Principle:
Purpose limitations

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

What this means:

When collecting personal data of any kind it must be for a specific purpose and the individual should be informed of what exactly that purpose is (in order to satisfy Principle 1). Unless there is a legal requirement to do so, this data must not be used for any other purpose without the consent of the data subject.

Case Study 2:

A States Member holds personal data of the members of his/her Committee, plus the details of many of his constituents on his computer for the purposes of discharging his duties as a

government official.

This States Member also has a new business selling CDs and DVDs on-line. He has all the e-mail addresses of his members and of most of his constituents and decides it would be a good business drive to send out marketing e-mails to all the people on his database to drum up some new business. He gets no reply from any so sends them out again. He continues to do this every day until the next meeting.

At the next meeting, all the members complain about receiving these e-mails and ask him to stop. The States Member has clearly breached the second principle as he is not registered to send marketing mail about another business to his colleagues and constituents. He would need to register his company separately and wear his company 'hat' to market people. Even then, he would need consent from his constituents and colleagues before processing their data in this manner.

Third Principle:
Adequate and relevant

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

What this means:

This requires the data controller to ensure that the information processed is relevant bearing in mind the purpose of collection.

Case Study 3:

A States Member held personal details of an individual claiming housing welfare. In order to pursue the claim, all that was needed from the individual was their name, address and date and place of birth. The States Member, however, asked the individual to provide personal details far in excess of what was required to pursue the claim.

This would constitute a breach of the third principle and any

personal data requested by the States Member from the individual must be relevant for the purposes of the claim, and not excessive for those purposes.

Fourth Principle:
Accurate and up to date

Personal data shall be accurate and, where necessary, kept up to date.

What this means:

Inaccurate and out-of-date information is of little use to anyone and may even be dangerous (for example in the case of medical information). It is therefore important to ensure high levels of accuracy as well as a method of updating information should it become out-dated.

It is vital to ensure that the information held about individuals is both accurate and kept up to date. If information becomes out of date, then this can lead to incorrect decisions being made about those individuals or the provision of sub-standard services.

Case Study 4:

The accuracy of the Electoral Roll can only be guaranteed by the Registrar-General of Electors who has the responsibility of maintaining that data. People move house regularly, and it is fair to assume that it would take very little time for the register to become inaccurate and out of date.

It is for this very reason that the onward processing of data obtained from the electoral roll can be dangerous, whether or not that data has been obtained fairly and lawfully.

Fifth Principle:
Held no longer than necessary

Personal data held for any purpose or purposes shall not be kept longer than is necessary for that purpose or those purposes.

What this means:

It is necessary to ensure that if holding information that has been sourced from a States department it is clear what the retention period relating to that data is and that this is adhered to.

Where the Members has themselves collected the data it is necessary to ensure that data which is no longer required is destroyed and that there are clear policies with regards to this. The more sensitive the data is, the more care needs to be taken with the methods of destruction.

Case Study 5:

Similarly to Case Study 4, personal data obtained from the Electoral Roll should not be kept for longer than is necessary for the purpose for which it was originally obtained, i.e. for the purposes of public elections.

If a States Member used historical electoral data, then it is likely that they would breach the fifth principle, as they have clearly kept it for longer than was necessary to fulfil the purpose for which it was **originally** obtained, eg. the previous election campaign.

Note: In this scenario, the States Member may also breach the fourth principle as the accuracy of that data cannot be guaranteed.

Sixth Principle:
Data subject rights

Personal data shall be processed in accordance with the rights of data subjects under this Law.

What this means:

Individuals have certain rights as provided in this Law. Those rights are detailed below.

States Members registered with the Commissioner carry with them the same obligations as any other data controller.

As such, all individuals who are the subjects of personal data held by a States Member have rights under the Law. Broadly, these are:

- Rights of access to personal data held about them;
- Rights to stop processing that causes damage or distress;
- Rights to stop processing for direct marketing purposes;
- Rights in relation to automated decision making;
- Rights to compensation from a data controller for damage and distress (upon application to the Court);
- Rights to have personal data rectified, blocked, erased or destroyed (upon application to the Court).

Where a data subject exercises rights under the Law, the data controller is expected to comply with that request, unless an exemption under the Law can be claimed.

Case Study 6:

A States Member holds a database on their computer of all constituents of a Parish district. One of the constituents that did not vote for this States Member is unhappy that this politician is holding personal details about them and decides to submit a subject access request to that States Member to establish exactly what information is held by him.

The States Member upon receiving the request thinks of it as a nuisance and disposes of the letter in the nearest bin.

The Law requires that a data controller, given sufficient information, has up to 60 days to respond to such a request. Failure to do so may result in the Court ordering the States Member to comply with the request.

Seventh Principle:
Security

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

What this means: It is important that all information held and processed is done so in a secure manner. All those with access to the States network will have signed up to the States policy in this respect.

States Members should have policies in place to ensure personal data for which they are the data controller is held securely.

Case Study 7:

A States Member holds a large amount of information on his home computer relating to constituents who are claiming welfare. The home computer is shared by his wife and their three teenage children. All the family use the computer on a daily basis and there are no password protected areas in the computer's hard drive. Essentially, the whole family have access to all areas of the computer, including the Parish welfare data.

One evening, the States Member's youngest son sends an e-mail to all his school friends, but instead of attaching a document containing an advert for the school magazine, he attaches the database containing details of all constituents claiming welfare.

In this example, the States Member as the data controller is responsible for ensuring the safeguard of the personal data held by him. This means that he must ensure that there are appropriate technical measures in place to safeguard that data, for example, password protection for those files containing this type of data.

In the case of an organisation holding personal data, which could be legitimately accessed by numerous members of staff, that organisation would also be expected to have appropriate organisational measures in place to safeguard the data, for example, robust policies and procedures governing the handling and processing of that data.

Eighth Principle:
Overseas transfers

Personal data shall not be transferred to a country or territory outside the Bailiwick of Guernsey unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

What this means:

Data transfers to jurisdictions that do not have comprehensive data protection laws in force are now restricted. Whilst it does not prohibit such transfers, there are conditions that must be satisfied prior to any such movement of data.

This principle is extremely unlikely to affect States Members as there would be very few occasions, if any at all, where a States Member would need to transfer personal data to a country or territory outside the Bailiwick of Guernsey.

Should circumstances arise where this does become a necessity, the States Member must ensure that the territory concerned ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the way that data is processed. A list of 'adequate' territories can be found on the European Commission website: www.europa.eu.int or alternatively you can seek advice from the Commissioner.

Frequently Asked Questions

Q. I only process information as a member of a Committee, do I need to notify?

A. It is likely that the processing will be covered by the Authority's notification. As long as no processing is taking place outside of that Committee there will be no need to notify.

Q. What is a data subject?

A. A data subject is an individual who is the subject of personal data.

Q. What is a data controller?

A. A data controller is the person or persons who control the manner in which data is collected and used. They are required to notify with the data protection authority.

Q. What is personal data?

A. Personal data is information that can identify an individual. (Please refer to Appendix 1 for processing conditions for personal data)

Q. What is sensitive personal data?

A. Sensitive personal data is information as to –

- racial, ethnic origin
- political opinions
- religious or other beliefs
- physical or mental health
- sexual life
- commission or alleged commission of any offence
- proceedings for any offence

(Please refer to Appendix 2 for processing conditions for sensitive personal data)

Q. I am notified in my own right and have a P.A. that deals with my administration. Can that P.A. access the information I hold?

A. A P.A. will act as a servant or agent of the data controller (the notified person) in the same way as an employee of an organisation would do. It is important that all staff appreciate their legal obligations in relation to the handling of all personal data. The data controller is responsible for compliance.

Q. I have been approached by a Parishioner to act on their behalf in dealings with a States entity. Is that organisation allowed to provide me with information pertinent to the enquiry?

A. The organisation is able to deal with persons acting for and on behalf of the data subject but it is unlikely that they will do so without formal authorisation from the data subject themselves. It is therefore helpful, when you are approached by the Parishioner, to ask that they include such an authority within their letter to you.

Q. I have been sent correspondence relating to an important political issue. Within it are a number of references to third parties. Can I disclose that to other Members or third parties?

A. The least problematic approach is to seek consent from the individuals concerned. If that proves impossible, the document should be anonymised. The greater the sensitivity of the information, the greater risk there is by disclosing. Advice should be sought.

Appendix 1

SCHEDULE 2

CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF ANY PERSONAL DATA

1. The data subject has given his consent to the processing.

2. The processing is necessary –

    (a) for the performance of a contract to which the data subject is a party, or

    (b) for the taking of steps at the request of the data subject with a view to entering into a contract.

3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4. The processing is necessary in order to protect the vital interests of the data subject.

5. The processing is necessary –

    (a) for the administration of justice,

    (b) for the exercise of any functions conferred on any person by or under any enactment,

    (c) for the exercise of any functions of the Crown, a Law Officer of the Crown [, a department of the States or a committee of the States of Alderney or the Chief Pleas of Sark], or

    (d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

6. (1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted

in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

(2) The Committee may by Order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

Appendix 2

SCHEDULE 3

CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF SENSITIVE PERSONAL DATA

1. The data subject has given his explicit consent to the processing of the personal data.

2. (1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

(2) The Committee may by Order –

(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

3. The processing is necessary –

(a) in order to protect the vital interests of the data subject or another person, in a case where –

(i) consent cannot be given by or on behalf of the data subject, or

(ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or

(b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4. The processing –

(a) is carried out in the course of its legitimate activities by any body or association which –

(i) is not established or conducted for profit, and

(ii) exists for political, philosophical, religious or trade-union purposes,

(b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,

(c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and

(d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6. The processing –

(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

(b) is necessary for the purpose of obtaining legal advice, or

(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7. (1) The processing is necessary –

(a) for the administration of justice,

(b) for the exercise of any functions conferred on any person by or under an enactment, or

(c) for the exercise of any functions of the Crown, a Law Officer of the Crown [, a department of the States or a committee of the States of Alderney or the Chief Pleas of Sark].

(2) The Committee may by Order –

(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

8. (1) The processing is necessary for medical purposes and is undertaken by –

(a) a health professional, or

(b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

(2) In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9. (1) The processing –

(a) is of sensitive personal data consisting of information as to racial or ethnic origin,

(b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and

(c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

(2) The Committee may by Order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

10. The personal data are processed in circumstances specified in an Order made by the Committee for the purposes of this paragraph.

Contact the Commissioner

Enquiries and Publication Requests

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