OFFICE OF THE INFORMATION COMMISSIONER

GUIDANCE:

GUIDANCE FOR STATES MEMBERS

OFFICE OF THE INFORMATION COMMISSIONER

Guidance Note

Guidance for States Members

Data Protection (Jersey) Law 2018

CONTENTS

Table of Contents

Introduction

The Data Protection (Jersey) Law 2018 ('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 must register with the Office of the Information 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 registration, 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 Register?

Acting on behalf of a Committee/Ministry or Department?

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

States Members who sit on a Committee or Ministry, or work directly with a Department (eg as a Minister or Assistant Minister) are likely to have access to and process personal information held at departmental level in the same way as civil service employees.

In such a situation, the data controller is the Committee/Ministry or Department rather than the member. The Committee/Ministry or Department is, therefore, legally responsible for the information and potentially liable for any breach.

An example is the Minister for Home Affairs who has access to driving licence files for the purpose of considering whether or not the Authority should proceed with the revocation of a driving licence. In this case the elected member is not required to register as the processing will be on behalf of the Department.

Acting on own behalf?

Members processing personal information to act on their own behalf, i.e. in the course of their constituency casework, will need to register in their own right. Examples include using personal information to timetable surgery appointments or progress complaints or enquiries made by local residents.

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

The 6 Data Protection Principles

States Members must also comply with six data protection principles, which together form an enforceable framework for the proper handling of personal data.

First Principle:
Processing is fair, lawful and transparent

Personal information shall be processed fairly, lawfully and in a transparent manner.

With regards to lawful processing, States members must have a lawful basis for which they are processing personal information. These are detailed in Schedule 2 of the Law (see Appendix 1).

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 departments. 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 the lawful basis for processing from one of the relevant conditions in Schedule 2 (depending on whether it is personal data or special category (sensitive) data that is being processed). Please refer to Appendix 1 for details of the conditions.

Case Study 1:

The Electoral Roll is prepared in each Parish in accordance with the requirements of the Public Elections (Jersey) Law 2002 ('the Public Elections Law'). It contains personal information relating to those Parish residents who are eligible to vote.

The Public Elections Law requires the Connetable of each Parish to make the register available for public inspection at each Parish Hall, the Judicial Greffe and the States Library. Copies of the register can be made to persons standing for election **once the nominations have been made**. Furthermore, the register must only be used for election purposes.

It is therefore not permitted for a States Member to either use, or obtain copies of the electoral register information 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 information shall be collected only for specified, explicit and legitimate purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

What this means:

When collecting personal information 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 information of the members of his/her Committee/Ministry or Department, plus the details of many of their constituents on his computer for the purposes of discharging their duties as a government official.

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

At the next meeting, all the members complain about receiving these e-mails and ask the States Member to stop. The States Member has clearly breached the second principle as they are not registered to send marketing mail about another business to their colleagues and constituents, nor have they sought permission from those people to use their information for that purpose.

The States Member would need to register their company separately and wear their company 'hat' to market people. Even then, they would need consent from their constituents and colleagues before processing their data in this manner.

Third Principle:
Adequate, relevant and limited

Personal data shall be adequate, relevant and limited to what is necessary 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, and follows a minimalist approach. This means collecting only what you need for the purposes you are collecting it for.

Case Study 3:

A States Member holds 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 limited to those purposes.

Fourth Principle:
Accurate and up to date

Personal data shall be accurate and, where necessary, kept up to date, with reasonable steps being taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

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.

As a States Member, it is your responsibility to ensure the accuracy of the information you hold, and to ensure any inaccurate information you hold is corrected swiftly.

Case Study 4:

The accuracy of the Electoral Roll can only be guaranteed by the Parish who have 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 Electoral Roll cannot be considered a reliable source of information for further use for purposes outside of the election process. Secondary 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 kept in a form that permits identification of data subjects must not be kept longer than is necessary for that purpose or those purposes.

What this means:

It is necessary to ensure that if holding personally identifiable 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. The States Department should have clear retention schedules setting out how long this information can be kept for.

Where the States Member 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.

The purpose of this Principle is to ensure that you only retain the information you need, and that it is disposed of appropriately once it is no longer required. It promotes good 'housekeeping', as well as minimising the risks of holding personal information unlawfully, insecurely, or using information which may no longer be accurate.

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 security

Personal data shall be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures.

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. It is likely (and in some cases advisable) that these policies reflect the Corporate States of Jersey Information Security policies, and you should make yourself fully aware of these.

As a States Member often holding highly sensitive personal information about constituents, the importance of maintaining robust security measures to protect the information you hold cannot be understated.

Case Study 7:

A States Member holds a large amount of information on his home computer relating to constituents who are claiming Parish 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 Parish welfare.

In this example, the States Member as the data controller is responsible for ensuring the security 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.

Overarching Principle:
Accountability and Transparency

As a States Member, you have been elected into a privileged position of power and trust. It is of utmost importance therefore that you lead by example and demonstrate a high level of integrity in relation to the personal information with which you are entrusted.
As a Data Controller, you should therefore be mindful of the overarching Principles of data protection law, including those of accountability for your actions in respect of personal information, and transparency in terms of how you process personal information.

Frequently Asked Questions

Q. I only process information as a member of Committee/Ministry or Department, do I need to register?

A. It is likely that the processing will be covered by the Committee/Ministry's registration. As long as no processing is taking place outside of that Committee/Ministry or Department there will be no need to register. However, the likelihood is you will also be processing personal information in relation to your constituency casework, and as such you will need to register.

Q. What is a data subject?

A. A data subject is an identified, or identifiable natural living person who can be identified, directly or indirectly, by reference to (but not limited to) an identifier such as:

a) A name, identification number or location data;
b) An online identifier;
c) One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the person.

The data subject is the individual who is the subject of personal data.

Q. What is a data controller?

A. A data controller is the natural or legal person or persons, public authority, agency or other body that, whether alone or jointly with others, determine the purposes and means of the processing of personal data.

The data controller is the organisation who control the manner in which data is collected and used. They are required to register 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 Special Category data?

A. Special Category personal data is information as to –

- racial, ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic or biometric data
- physical or mental health
- sexual life or sexual orientation
- criminal record data or alleged criminal activity.

(Please refer to Appendix 1 for processing conditions for Special Category data)

Q. I am registered 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 registered 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 Department. Is that Department allowed to provide me with information pertinent to the enquiry?

A. The Department 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. There may also be a more valid or relevant 'condition for processing' available under Schedule 2 of the Law (see Appendix 1) which can be applied to the circumstances. The greater the sensitivity of the information, the greater risk there is by disclosing. Advice should be sought.

Appendix 1

SCHEDULE 2
(Article 9)
CONDITIONS FOR PROCESSING

PART 1 – CONDITIONS FOR PROCESSING PERSONAL DATA

1 Consent
The data subject has consented to the processing of his or her data for one or more specific purposes.

2 Contract
The processing is necessary for –
(a) the performance of a contract to which the data subject is a party; or
(b) the taking of steps at the request of the data subject with a view to entering into a contract.

3 Vital interests
The processing is necessary to protect the vital interests of the data subject or any other natural person.

4 Public functions
The processing is necessary for –
(a) the administration of justice;
(b) the exercise of any functions conferred on any person by or under any enactment;
(c) the exercise of any functions of the Crown, the States or any public authority; or
(d) the exercise of any other functions of a public nature with a legal basis in Jersey law to which the controller is subject and exercised in the public interest by any person.

5 Legitimate interests
(1) The processing is necessary for the purposes of legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, unless –
(a) the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject, in particular where the subject is a child; or
(b) the controller is a public authority. Data Protection (Jersey) Law 2018
(2) The States may by Regulations specify particular circumstances in which the condition set out in sub-paragraph (1)(a) is, or is not, to be taken to be satisfied.

PART 2 – CONDITIONS FOR PROCESSING PERSONAL DATA AND SPECIAL CATEGORY DATA

6 Consent
The data subject has given explicit consent to the processing for one or more specific purposes.

7 Other legal obligations
The processing is necessary for compliance with a legal obligation, other than one imposed by contract, to which the controller is subject.

8 Employment and social fields
The processing is necessary for the purposes of exercising or performing any right, obligation or public function conferred or imposed by law on the controller in connection with employment, social security, social services or social care.

9 Vital interests
The processing is necessary in order to protect the vital interests of –
(a) the data subject or another person, in a case where consent cannot be given by or on behalf of the data subject, or the controller cannot reasonably be expected to obtain the consent of the data subject; or
(b) another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

10 Non-profit associations
The processing –
(a) is carried out in the course of its legitimate activities by any body, or association, that is not established or conducted for profit, and 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 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.

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

12 Legal proceedings, etc.
The processing is necessary for the purposes of –
(a) any legal proceedings;
(b) obtaining legal advice; or
(c) establishing, exercising or defending legal rights.

13 Public functions
The processing is necessary for –
(a) the administration of justice;
(b) the exercise of any functions conferred on any person by or under an enactment; or
(c) the exercise of any functions of the Crown, the States, any administration of the States or any public authority.

14 Public interest
The processing is necessary for reasons of substantial public interest provided for by law and is subject to appropriate protections to protect the rights and interests of the data subject.

15 Medical purposes
(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 equivalent to that which would arise if that person were a health professional.

(2) In paragraph (1) "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment, the management of healthcare services, occupational medicine and the assessment of the working capacity of the employee.

16 Public health

The processing is necessary for reasons of public interest in the area of public health, including (but not limited to) protecting against cross border threats to health and ensuring a high standard of quality and safety of health care or social care where they are provided for by law and the processing is carried out with appropriate safeguards for the rights and freedoms of data subjects.

17 Archiving and research

The processing –
(a) is in the public interest;
(b) is necessary for the purposes of archiving or for statistical, scientific or historical research;
(c) does not support measures or decisions with respect to any particular data subject otherwise than with the explicit consent of the data subject; and
(d) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

18 Avoidance of discrimination

(1) The processing –
(a) consists of information as to –
(i) any protected characteristic within the meaning of the Discrimination (Jersey) Law 2013[35], or
(ii) a person's disability, or
(iii) a person's religious beliefs;
(b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment of persons on grounds of any characteristic described in clause (a)(i) to (iii) with a view to enabling such equality to be promoted or maintained;
(c) does not support measures or decisions with respect to any particular data subject otherwise than with the explicit consent of the data subject; and
(d) is carried out with appropriate safeguards for the rights and freedoms of data subjects.
(2) The processing is not contrary to any notice in writing that an individual has given to the controller requiring the controller to cease processing personal data in respect of which the individual is the data subject, such notice taking effect at the end of a period that is reasonable in the circumstances or, if longer, the period specified in the notice.

19 Prevention of unlawful acts

The processing –
(a) is in the substantial public interest;
(b) is necessary for the purposes of the prevention or detection of any unlawful act or unlawful omission; and
(c) in order not to prejudice those purposes, is required to be carried out without the controller's seeking the explicit consent of the data subject.

20 Protection against malpractice and mismanagement

The processing –
(a) is in the substantial public interest;

(b) is necessary for the discharge of any function that is designed for protecting members of the public against –
(i) dishonesty, malpractice, or other seriously improper conduct by, or the unfitness or incompetence of, any person, or
(ii) mismanagement in the administration of, or failures in services provided by, any body or association; and
(c) in order not to prejudice the discharge of that function, is required to be carried out without the controller's seeking the explicit consent of the data subject.

21 Publication about malpractice and mismanagement
(1) The processing –
(a) takes the form of disclosure;
(b) is in the substantial public interest;
(c) is in connection with –
(i) the commission by any person of any unlawful act, or unlawful omission, whether alleged or established,
(ii) dishonesty, malpractice, or other seriously improper conduct by, or the unfitness or incompetence of, any person, whether alleged or established, or
(iii) mismanagement in the administration of, or failures in services provided by, any body or association, whether the mismanagement or failures are alleged or established;
(d) is for the special purposes; and
(e) is made with a view to the publication of those data by any person.
(2) The person who is the controller in relation to the processing reasonably believes that the publication would be in the public interest.

22 Counselling
(1) The processing –
(a) is in the substantial public interest; and
(b) is necessary for the discharge of any function designed for the provision of confidential counselling, confidential advice, confidential support or a similar confidential service.
(2) One or more of the following conditions is satisfied –
(a) the data subject cannot give consent to the processing;
(b) the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;
(c) the processing must, in order not to prejudice the discharge of the function referred to in sub-paragraph (1)(b), be carried out without the controller's seeking the explicit consent of the data subject.

23 Insurance and pensions: general determinations
(1) The processing –
(a) is necessary for the purpose of –
(i) carrying on insurance business falling within Class I, III or IV of Part 1 of Schedule 1 to the Insurance Business (Jersey) Law 1996[36], or within Class 1 or 2 of Part 2 of that Schedule, or
(ii) making determinations in connection with eligibility for, or benefits payable under, an occupational pension scheme, being a scheme, or arrangement, that is constituted in one or more instruments or agreements and has, or is capable of having, effect in relation to one or more descriptions or categories of employments so as to provide benefits, in the form of pensions or otherwise, payable on termination of service, or on death or retirement, to or in respect of earners with qualifying service in an employment of any such description or category; and

(b) does not support measures or decisions that relate in particular to the person who is the data subject in respect of the personal data.
(2) The controller cannot reasonably be expected to obtain the explicit consent of that data subject to the processing and the controller is not aware of the data subject's withholding his or her consent to the processing.
(3) The personal data consists of information relating to the physical or mental health or condition of a data subject who is the parent, grandparent, great-grandparent or sibling of –
(a) in the case of processing for the purpose referred to in sub-paragraph (1)(a)(i), a person insured (or seeking to be insured) in the course of the insurance business; or
(b) in the case of processing for the purpose referred to in sub-paragraph (1)(a)(ii), a person who is a member of the scheme or seeking to become a member of the scheme.

24 Insurance and pensions: current processing
(1) The processing –
(a) was already under way in relation to the same data subject and by or on behalf of the same controller immediately before the coming into force of this Schedule; and
(b) is necessary for the purpose of –
(i) carrying on insurance business falling within Class I, III or IV of Part 1 of Schedule 1 to the Insurance Business (Jersey) Law 1996, or
(ii) establishing or administering an occupational pension scheme, being a scheme, or arrangement, that is constituted in one or more instruments or agreements and has, or is capable of having, effect in relation to one or more descriptions or categories of employments so as to provide benefits, in the form of pensions or otherwise, payable on termination of service, or on death or retirement, to or in respect of earners with qualifying service in an employment of any such description or category.
(2) One or both of the following conditions is satisfied –
(a) the controller cannot reasonably be expected to obtain the explicit consent of the data subject to the processing and has not been informed by the data subject that the latter refuses consent to the processing;
(b) the processing must, in order not to prejudice the purpose referred to in sub-paragraph (1)(b), be carried out without the controller's seeking the explicit consent of the data subject.

25 Functions of a police officer
The processing is necessary for the exercise of any function conferred on a police officer by or under any enactment or other law.

26 Regulations
Regulations may –
(a) specify further circumstances in which special category data are processed;
(b) exclude the application of this Schedule in such cases as may be specified;
(c) provide that, in such cases as may be specified, any condition in this Schedule is not to be regarded as satisfied unless such further conditions as may be specified in the Regulations are also satisfied; or
(d) specify circumstances in which processing falling within paragraph 17(a) and (b) is, or is not, to be taken for the purposes of paragraph 17(d) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

Contact the Commissioner

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

T: +44 (0)1534 716530
W: www.oicjersey.org
E: enquiries@oicjersey.org

MORE INFORMATION

Additional guidance is available on our guidance pages with more information on other aspect of the DPJL.

This guidance has been developed drawing on the Commissioner's experience. It will be reviewed and considered from time-to-time in line with new decisions by the Commissioner and/or the Jersey courts.

It is a guide to our general recommended approach, although each individual case will likely be different and will be decided on the particular circumstances of the case.

If you need any further information about this, or any other aspect of the DPJL, please contact us or see our website www.oicjersey.org.

OFFICE OF THE INFORMATION COMMISSIONER