JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

GUIDANCE NOTE

The Data Protection Principles

Data Protection (Jersey) Law 2018

MAY 2018 • V1 • WWW.JERSEYOIC.ORG

CONTENTS

Introduction 3

The Data Protection Principles 4

Schedule 2: Conditions for processing of personal data 9

More information 15

INTRODUCTION

1. This guidance relates to the Data Protection (Jersey) Law 2018 (the **DPJL**).

2. The DPJL is based around six principles of 'good information handling' (the **Principles**). These principles give people (the data subjects) specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it.

3. This is part of a series of guidance, which goes into more detail than the Guide, to help organisations fully understand their obligations, as well as to promote good practice.

4. This guidance aims to provide explanations about the Principles, to help individuals understand their rights and to provide guidance to organisations about how they must process data in accordance with those Principles.

THE DATA PROTECTION PRINCIPLES

The Principles are at the core of the responsibilities placed upon controllers and processors. Whilst compliance with each Principle must be met, they are inextricably linked and therefore should not be read in isolation.

A controller must ensure that the processing of personal data in relation to which the controller is the controller complies with the data protection principles (Article 8 DPJL), namely:

Fair, lawful and transparent processing:

Personal data are to be processed lawfully, fairly and in a transparent manner in relation to the data.

NOTES:

Lawful processing

- To ensure lawful processing of personal data, the controller or processor must meet at least one of the conditions specified in Schedule 2 (see page 86). No single basis is better or more important than the others – which basis is most appropriate to use will depend on the organisation's purpose and relationship with the individual. At least one of these must apply wherever an organisation processes personal data:
    - » Consent: the individual has given clear consent for an organisation to process their personal data.
    - » Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
    - » Legal obligation: the processing is necessary to comply with the law (not including contractual obligations).
    - » Vital interests: the processing is necessary to protect someone's life.
    - » Public task: the processing is necessary for the performance of a task in the public interest, or for official functions, and the task or function has a clear basis in law.
    - » Legitimate interests: the processing is necessary for the organisation's legitimate interests or the legitimate interests of a third party unless there is good reason to protect the individual's personal data which overrides those legitimate interests. (This doesn't apply to public authorities processing data to perform official tasks.)
- However, in the case of any processing of data that includes special category data, it must also meet at least one of the conditions mentioned in Part 2 of Schedule 2 (see page 9).
- An organisation must determine the lawful basis before processing begins and it should be documented. The basis for processing should be documented in any privacy notice.
- For more information on the legal bases for processing data see our related guidance note.

Fair and transparent processing

- To ensure your processing is fair and transparent, controllers and processors must consider how the data are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purposes for which they are to be processed.
- Personal data are regarded as obtained fairly if they consist of information obtained from a person who –
  - » is authorized by law to supply it; or
  - » is required to supply it by law or any international agreement imposing an international obligation on Jersey.
- In order that personal data may be processed fairly and transparently, a controller must –
  - » facilitate the exercise of the rights of data subjects;
  - » act on a data subject's request unless the data subject cannot be identified from the data or the processing is exempted.

Purpose limitation:

Personal data must be collected for specified, explicit and legitimate purposes and once collected, not further processed in a manner incompatible with those purposes.

NOTES:

This means controllers and processors cannot obtain personal data for one purpose and then go on to use it for another incompatible purpose. Every new purpose must have its own legal basis and the purpose must be defined before processing is started.

Example 1

A ferry company collects data from its passengers in order to make bookings and so that it knows how many people are travelling with them. The ferry company will need information regarding the passenger's seat number, registration of any vehicle, any special physical needs. If the ferry company are asked to pass this information on to Customs and Immigration, then the information is then being used for a different purpose from that for which it was originally collected. Transfer of the data to Customs and Immigration would need a new and separate legal basis, which the company would need to document.

Further processing for the purposes archiving and research is not considered as incompatible with the initial purposes for which the data was collected.

Excessive data collection:

Personal data collected must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

NOTES:

This Principle is to ensure compliance with the concept of data minimisation, meaning that controllers and processors should only collect personal data that is sufficient for the purposes for which it is required. You should identify the minimum amount of personal data you need to properly fulfil your purpose. You should hold that much information but no more than that and you should not keep information simply on the basis that it might be useful in the future but where you have no actual need for it.

In order to assess whether you are holding the right amount of personal data, you will have to be clear about why you are holding and using it.

Example 2

A debt collection agency is engaged to find a particular debtor. It collects information on several people with a similar name to the debtor. During the enquiry some of these people are discounted. The agency should delete most of their personal data, keeping only the minimum needed to form a basic record of a person they have removed from their search. It is appropriate to keep a small amount of information so that these people are not contacted again about debts which do not belong to them.

Where special category data is concerned it is particularly important to make sure that only the minimum amount of information is collected as is necessary.

Example 3

A recruitment agency places workers in a variety of jobs. It sends all applicants (regardless of the job applied for) a questionnaire which includes questions about health conditions that are only relevant to particular manual occupations. It would be irrelevant and excessive to obtain such information from all individuals, regardless of the job they were actually applying for.

Example 4

An employer holds details of the blood groups of all its employees. Some of the workers do hazardous work and the information is needed in case of an accident. For the rest of the workforce, holding such information is likely to be irrelevant and excessive.

Accuracy of data:

Personal data must 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.

NOTES:

This Principle requires controllers and processors to take steps to ensure the continued accuracy of the personal data they hold. This might be through routine interactions with customers, certain trigger events or an annual review of customer databases. If the information is used for a purpose that relies on it remaining current, it should be kept up to date i.e. employee payroll records should be updated when an employee receives a pay rise.

It also requires that controllers and processors erase or amend any personal data that is found to be inaccurate without delay.

Storage limitation:

Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed.

NOTES:

This Principle relates to the retention of personal data and requires that controllers and processors do not retain personal data for longer than is necessary for the purposes for which it was obtained. The Law does not set out any specific minimum or maximum periods for retaining personal data; it is for the organisation to assess how long they need to keep the data for, and why. Ensuring personal data is disposed of when no longer needed will reduce the risk that it will become inaccurate, out of date or irrelevant.

It only relates to personal data that allows for the identification of individuals.

In assessing what is 'no longer than necessary', some controllers and processors may be subject to other statutory or regulatory instruments which set record keeping requirements for businesses in respect of certain data sets. Examples of this may include Anti-Money laundering legislation, Jersey contracts or medical council guidelines. These should be incorporated into your retention policies.

Where no statutory or regulatory instruments governing record keeping requirements are applicable, controllers and processors will need to establish their own reasonable retention periods considering all the circumstances of the processing.

Personal data may be stored to the extent necessary for the purposes of satisfying legal obligations imposed upon the organisation, and for archiving and research purposes as long as those data sets are subject to the appropriate technical and organisational security measures required by the 6th Data Protection Principle.

Organisations will need to:

- Review the length of time they keep personal data;
- Consider the purpose or purposes they hold the information for in deciding whether (and for how long) to retain it;
- Securely delete information that is no longer needed for this purpose or these purposes; and
- Update, archive or securely delete information if it becomes out of date.

Data security, integrity and confidentiality:

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

NOTES:

This Principle requires controllers and processors to ensure the appropriate technical and organisational measures are in place to protect the personal data they hold. This means the development of robust data security systems and confidentiality policies and procedures. It also means training staff to ensure they know how to keep personal information safe.

'Technical measures' will include measures such as access restrictions to certain files, password protections, firewalls, virus and malware protections, and protections from external cyber-attacks, among others.

'Organisational measures' will include policies and procedures for staff. Some of those policies might include (but are not limited to) the following:

- Clear desk policy
- Acceptable email and internet use policy
- Policies for remote network access and use of mobile devices/removable external data storage devices
- Building/office security and access restrictions
- Data security policies: Removing, altering data; sending emails to unsecure email addresses; removal of data from the business premises; taking client data when leaving the organisation
- Opening emails/attachments from untrusted sources/websites
- Identifying and reporting data breaches.

SCHEDULE 2: CONDITIONS FOR PROCESSING OF PERSONAL DATA

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.
   (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; or

(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.

MORE INFORMATION

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

6. 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.

7. 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.

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

Jersey Office of the Information Commissioner
2nd Floor
5 Castle Street
St Helier
Jersey JE2 3BT

Telephone number: +44 (0) 1534 716530
Email: enquiries@jerseyoic.org