



**OFFICE OF THE
INFORMATION
COMMISSIONER**

The Data Protection Principles

Data Protection (Jersey) Law 2005

Table of Contents

Introduction	2
First Principle	2
Second Principle	5
Third Principle	6
Fourth Principle	6
Fifth Principle	7
Sixth Principle	7
Seventh Principle	7
Eighth principle	9
Contact the Commissioner	17

Introduction

Schedule 1 of the Data Protection (Jersey) Law 2005 (“the Law”) provides for eight enforceable Principles of data protection, which form the bedrock of the legislation and control the manner in which personal data is handled. All persons processing personal data are expected to comply with these Principles.

This guidance document details each of the eight Principles and provides notes on how to interpret them.

First Principle

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

- (a) in every case – at least one of the conditions set out in paragraphs 1-6 of Schedule 2 (*see Appendix 1*) is met; and
- (b) in the case of sensitive personal data– at least one of the conditions in paragraphs 1-10 of Schedule 3 (*see Appendix 2*) is also met.

INTERPRETATION:

1 First principle: source

- (1) In determining for the purposes of the first principle whether personal data are processed fairly, regard is to be had to the method by which they are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be processed.
- (2) Subject to paragraph 2, for the purposes of the first principle data are to be treated as obtained fairly if they consist of information obtained from a person who –

- (a) is authorized by or under any enactment to supply it; or
- (b) is required to supply it by or under any enactment or by any convention or other instrument imposing an international obligation on Jersey.

2 First principle: specified information at relevant time

- (1) Subject to paragraph 3, for the purposes of the first principle personal data are not to be treated as processed fairly unless –
 - (a) in the case of data obtained from the data subject - the data controller ensures so far as practicable that the data subject has, is provided with, or has made readily available to him or her, the specified information; or
 - (b) in any other case - the data controller ensures so far as practicable that, before the relevant time or as soon as practicable after that time, the data subject has, is provided with, or has made readily available to him or her, the specified information.
- (2) For the purposes of this paragraph, the relevant time is –
 - (a) in any case – the time when the data controller first processes the data; or
 - (b) in a case where, at the time when the data controller first processes the data, disclosure of the data to a third party within a reasonable period is envisaged –
 - (i) if the data are in fact disclosed to a third party within a reasonable period – the time when the data are first disclosed,
 - (ii) if within that period the data controller becomes, or ought to become, aware that the data are

unlikely to be disclosed to such a person within that period – the time when the data controller does become, or ought to become, so aware, or

(iii) in any other case - the end of that period.

- (3) For the purposes of this paragraph, the specified information is all of the following –
- (a) the identity of the data controller;
 - (b) the identity of the representative (if any) nominated by the data controller under Article 5;
 - (c) the purpose or purposes for which the data are intended to be processed; and
 - (d) any further information that is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair.

3 First principle: primary and other conditions

- (1) Paragraph 2(1)(b) does not apply if either of the primary conditions, together with such further conditions as may be prescribed by Regulations, are met.
- (2) For the purposes of this paragraph, the primary conditions are –
- (a) that the provision of the specified information would involve a disproportionate effort on the part of the data controller; and
 - (b) that the recording of the information to be contained in the data by, or the disclosure of the data by, the data controller is necessary for compliance with any legal

obligation to which the data controller is subject, other than an obligation imposed by contract.

4 First principle: general identifier

- (1) For the purposes of the first principle, personal data that contain a general identifier falling within such description as may be prescribed by Regulations are not to be treated as processed fairly and lawfully unless they are processed in compliance with any conditions so prescribed in relation to general identifiers of that description.
- (2) In this paragraph, “general identifier” means any identifier (for example, a number or code used for identification purposes) that relates to an individual and forms part of a set of similar identifiers that is of general application.

Second Principle

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.

INTERPRETATION:

5 Second principle: how purpose specified

For the purposes of the second principle, the purpose or purposes for which personal data are obtained may in particular be specified

–

- (a) in a notice (if any) given for the purposes of paragraph 2 by the data controller to the data subject; or
- (b) in a notification given to the Commissioner under Part 3 of this Law.

6 Second principle: purpose of processing after disclosure

For the purposes of the second principle, in determining whether any disclosure of personal data is compatible with the purpose or purposes for which the data were obtained, regard is to be had to the purpose or purposes for which the personal data are intended to be processed by any person to whom they are disclosed.

Third Principle

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

Fourth Principle

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

INTERPRETATION:

7 Fourth principle

The fourth principle is not to be regarded as being contravened by reason of any inaccuracy in personal data that accurately record information obtained by the data controller from the data subject or a third party in a case where –

- (a) having regard to the purpose or purposes for which the data were obtained and further processed, the data controller has taken reasonable steps to ensure the accuracy of the data; and
- (b) if the data subject has notified the data controller of the data subject's view that the data are inaccurate – the data indicate that fact.

Fifth Principle

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

Sixth Principle

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

INTERPRETATION:

8 Sixth principle

A person is to be regarded as contravening the sixth principle if the person fails –

- (a) to supply information in accordance with Article 7;
- (b) to comply with a notice given under Article 10(1) to the extent that the notice is justified;
- (c) to give a notice under Article 10(3);
- (d) to comply with a notice given under Article 11(1);
- (e) to comply with a notice given under Article 12(1) or (2)(b);
or
- (f) to give a notification under Article 12(2)(a) or a notice under Article 12(3).

Seventh Principle

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

INTERPRETATION:

9 Seventh principle: appropriateness of measures

For the purposes of the seventh principle, the measures shall ensure, having regard to the state of technological development and the cost of implementing any measures, a level of security appropriate to –

- (a) the harm that might result from unauthorized or unlawful processing of, or accidental loss, destruction or damage to, the personal data; and
- (b) the nature of the personal data to be protected.

10 Seventh principle: reliability of employees

For the purposes of the seventh principle, the data controller shall take reasonable steps to ensure the reliability of any employees of the data controller who have access to the personal data.

11 Seventh principle: reliability of data processor

If processing of personal data is carried out by a data processor on behalf of a data controller, the data controller shall in order to comply with the seventh principle –

- (a) choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out; and
- (b) take reasonable steps to ensure compliance with those measures.

12 Seventh principle: processing contract to ensure reliability

If processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with the seventh principle unless the processing is carried out under a contract –

- (a) that is made or evidenced in writing;
- (b) under which the data processor is to act only on instructions from the data controller; and
- (c) that requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle.

Eighth Principle

Personal data shall not be transferred to a country or territory outside the European Economic Area 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.

INTERPRETATION:

13 Eighth principle: what is adequate protection in foreign country

For the purposes of the eighth principle, an adequate level of protection is one that is adequate in all the circumstances of the case, having regard in particular to –

- (a) the nature of the personal data;
- (b) the country or territory of origin of the information contained in the data;
- (c) the country or territory of final destination of that information;

- (d) the purposes for which and period during which the data are intended to be processed;
- (e) the law in force in the country or territory in question;
- (f) the international obligations of that country or territory;
- (g) any relevant codes of conduct or other rules that are enforceable in that country or territory (whether generally or by arrangement in particular cases); and
- (h) any security measures taken in respect of the data in that country or territory.

14 Exceptions to eighth principle

The eighth principle does not apply to a transfer falling within any of paragraphs 1-9 of Schedule 4, except in such circumstances and to such extent as may be prescribed by Regulations.

SCHEDULE 2

(Article 4(3) and Schedule 1 Part 1, paragraph 1(a))

**FIRST PRINCIPLE: CONDITIONS FOR PROCESSING OF ANY
PERSONAL DATA**

1 Consent

The data subject has consented to the processing.

2 Processing necessary for 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 Processing under legal obligation

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 Processing to protect vital interests

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

5 Processing necessary for exercise of 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 exercised in the public interest by any person.

6 Processing for legitimate interests

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

7 Regulations about legitimate interests

The States may by Regulations specify particular circumstances in which the condition set out in paragraph 6 is, or is not, to be taken to be satisfied.

SCHEDULE 3

(Article 4(3) and Schedule 1 Part 1, paragraph 1(b))

FIRST PRINCIPLE: CONDITIONS FOR PROCESSING OF SENSITIVE PERSONAL DATA

1 Consent

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

2 Employment

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

3 Vital interests

The processing is necessary –

- (a) in order to protect the vital interests of the data subject or another person, in a case where consent cannot be given by or on behalf of the data subject, or 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 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.

5 Data subject has made information public

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

6 Legal proceedings etc.

The processing –

- (a) is necessary for the purpose of, or in connection with, any 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 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.

8 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 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 Equal opportunity research

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.

10 Circumstances prescribed by Regulations

The personal data are processed in such circumstances as may be prescribed by Regulations.

11 Regulations about paragraph 2, 7 or 9

- (1) The States may by Regulations –
 - (a) exclude the application of paragraph 2 or 7 in such cases as may be specified; or
 - (b) provide that, in such cases as may be specified, the condition in paragraph 2 or 7 is not to be regarded as satisfied unless such further conditions as may be specified in the Regulations are also satisfied.
- (2) The States may by Regulations specify circumstances in which processing falling within paragraph 9(a) and (b) is, or is not, to be taken for the purposes of paragraph 9(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

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