OFFICE OF THE INFORMATION COMMISSIONER

Data Protection (Jersey) Law 2005 :

Code of Practice & Guidance on the Processing of Personal Data for Credit Purposes

For data controllers based in the Bailiwick of Jersey

Table of Contents

Introduction

This Code of Practice ('the Code') has been prepared by the Information Commissioner ('the Commissioner') in accordance with the powers contained within Article 51(3) of the Data Protection (Jersey) Law 2005 ('the Law'). This Code reflects the Commissioner's view regarding the processing of personal data for credit purposes. The Commissioner considers that processing personal data in otherwise than in accordance with this Code may breach the requirements of the principles of the Law.

Review

The Commissioner reserves the right to review and revise the Code in the light of practical experience of it operation, changes in technology, industry practice or the expectations of data subjects.

Scope

The Code applies to personal data, that is data relating to living individuals, processed for the purpose of providing credit and services or products.

The Code applies to any personal data processed in order to provide credit services or products, regardless of from where the information is sourced. As such it also covers the processing of personal data derived from publicly available sources.

The Code applies to all data controllers processing within the Bailiwick of Jersey for the purpose of providing credit and related services or products.

Definitions

Unless otherwise stated the definitions of the Data Protection (Jersey) Law 2005 apply.

1st Data Protection 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.*

Schedule 1, Part 2 of the Law provides interpretation of this principle – Appendix 3

In any case where data is not obtained directly from the data subject, the data controller should ensure the data subject is provided with information as to the identity of the data controller as well as details regarding the nature of the processing. The data controller should provide this information at the time when processing commences. Therefore, once a credit reference agency receives information relating to a data subject which they intend to process for commercial credit purposes, the individual who is the subject of that processing must be informed that the processing is underway.

At the time of collecting personal data related to credit applications / relationships, an organisation must inform the data subject of the processes involved and the use to which data shall be put within the framework of a credit information system and seek consent from the data subject for such processing. The information shall include a clear and accurate description of the purposes and mechanisms of any processing of data and shall also detail the particular credit reference agency being used. In the absence of clear consent from the data subject, the credit reference agency should not disclose any personal data for the purpose of providing credit and such services or products unless and until such consent is evidenced.

2nd Data Protection 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.*

The personal data contained in a credit information system may only be processed by the credit reference agency and the organisation using their services for the purpose of protecting credit and limiting any corresponding risks, and in particular, to assess the data subject's financial status and creditworthiness or, at least, their ability and reliability to make payments on time. The information should not be used for any other purposes including the promotion, advertising and/or direct selling of products or services unless specific consent has been provided by the data subject.

3rd Data Protection Principle

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

Only information directly and specifically relevant to the data controller's business functions should be collected, processed and disclosed.

The details contained in the Petty Debts Court Table, as published weekly by the Magistrate's Court Greffe, are only to be processed by the recipients of the document for the purposes of confirmation that their attendance or that of their clients may be necessary in relation to that Petty Debts Court session. Data contained in the Table document should not be further processed unless such processing is in compliance with Schedules 2 and 3 of the Law.

Where a judgment is made in the Petty Debts Court, judgment data should only be processed in accordance with the conditions set out in Schedules 2 and 3 of the Law.

4th Data Protection Principle

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

Data controllers must take all reasonable steps to ensure correct identification of, as well as accurate and up to date contact information for individuals. Procedures should be in place to deal with complaints concerning incorrect identification. Where there is doubt about the identification of an individual the system must flag the fact and further details should be sought from any organisation submitting a credit check request before a formal response is provided.

An individual who is subject of personal data processed by a data controller can notify that data controller of their view that the data are inaccurate. If the data controller has taken reasonable steps to ensure accuracy this principle will not be contravened as long as the file relating to the individual refers to the fact that the data are in dispute.

Where an individual informs a data controller that data is incorrect or should be deleted, the data controller should, within 28 days, notify the individual that the data has been amended or removed. In the event that the data controller has concluded that no action is required, the individual should be informed of that fact.

It should be noted that Guernsey judgements have no status and should only be shown as judgements, rather than outstanding judgements. This is due to there being no mechanism within the Guernsey court process to record the status of judgments or obtain a Certificate of Satisfaction.

5th Data Protection Principle

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

Personal data relating to judgments that have been taken against individuals may be retained for a maximum period from the date of the judgement as outlined below, determined by the jurisdiction in which the judgement was made.

Jurisdiction of Judgement	Maximum Retention Term
Jersey	10 years
Bailiwick of Guernsey	6 years
Other	6 years

Any judgment that has been set aside/abandoned should be removed from the systems of the data controller immediately any such action is publicly recorded, or within 14 days of this time where this is not practicable.

6th Data Protection Principle

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

With regard to the personal data recorded in a credit information or debt collection system, data subjects shall be entitled to exercise their rights in accordance with the mechanisms set out in the Law both in respect of the credit/debt collection agency and in respect of the organisations that have communicated the said data. A maximum fee of £10 may be requested for a full request covering all data held and such requests should be replied to as soon as possible and in any event within 40 days.

If the data requested is limited to personal data relevant to an individual's financial standing, a maximum fee of £2 may be requested and such requests should be replied to as soon as possible and in any event within 7 working days.

A credit reference agency that receives a request for information from the individual who is the subject of that information must provide that individual with a statement of rights as prescribed in the Schedule to the Data Protection (Credit Reference Agency)(Jersey) Regulations 2005 (see Appendix 4).

An individual is also entitled at any time to ask that no decision that significantly affects them is based solely on the processing by automatic means (automated decision-making). Article 12 of the Law applies in this respect.

7th Data Protection 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.*

This provision ensures that appropriate care is taken of personal data. For electronic processing, data controllers should consider appropriate measures to ensure data integrity, including the installation of virus protection software and firewalls, adopting encryption for data transfers, using privacy enhancing technologies and making regular backups that are stored securely. For manual processing, consideration should be given to appropriate security measures, such as storage of paper records in fire-proof, lockable cabinets. Access to any data should be strictly limited to those with a legitimate need and staff should be appropriately trained.

8th Data Protection Principle

> *Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.*

No personal data should be transferred outside of the European Economic Area unless the data controller can ensure the personal data will be subject to an adequate level of data protection in accordance with the requirements set out in the Law or where transfer is such that the 8th principle does not apply. These transfers are outlined in Schedule 4 of the Law (see Appendix 5).

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.

Appendix 2

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.

SCHEDULE 1

PART 2

(Article 4(2))

INTERPRETATION OF DATA PROTECTION PRINCIPLES

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.

Appendix 4

Data Protection (Credit Reference Agency) (Jersey) Regulations 2005

Made	*25th October 2005*
Coming into operation	*1st December 2005*

THE STATES, in pursuance of Articles 9(3) and 67 of the Data Protection (Jersey) Law 2005,[1] have made the following Regulations –

1 Interpretation

In these Regulations "Law" means the Data Protection (Jersey) Law 2005.

2 Statement of rights

(1) For the purposes of Article 9(3) of the Law the prescribed form is the matter set out in the Schedule together with the telephone numbers and website addresses for each of the services mentioned in paragraph 3 of the Schedule and with the address, telephone number and website address of the Commissioner.

(2) For the purposes of Article 9(3) of the Law the prescribed extent is in every case the full extent of the form prescribed in paragraph (1).

3 Citation and commencement

These Regulations may be cited as the Data Protection (Credit Reference Agency) (Jersey) Regulations 2005 and shall come into force on 1st December 2005.

SCHEDULE

(Regulation 2(1))

YOUR RIGHTS AS A DATA SUBJECT

You have the following rights which you can enforce through a court.

1 Right of subject access (Article 7)

This is the right to find out what information about you is held on computer and in some paper records.

2 Correcting inaccurate data (Principle 4 and Articles 13 and 14)

You have the right to have inaccurate personal data rectified, blocked, erased, or destroyed.

If you believe you have suffered damage or distress as a result of the processing of inaccurate data you can ask the court to award you compensation.

3 Preventing direct marketing (Article 11)

You have the right to request in writing that a data controller not use your personal data for direct marketing by post (sometimes known as junk mail), by telephone or by fax.

Your request must be complied with. There are no exceptions to this.

You can also register with the mailing preference service, the telephone preference service and the fax preference service.

Once you have done this you should not receive any direct marketing from the United Kingdom unless you have asked for it or you are an existing customer of an organization.

4 Preventing automated decision-making (Article 12)

You can write to a data controller to ask that he or she not take any decision that significantly affects you based solely on an automated process. For example, many banks have a computerized system of credit scoring.

Where a decision has already been taken on this basis you can ask the data controller to reconsider or to use a different method to make the decision.

5 Preventing processing that may cause damage or distress (Article 10)

If you think that certain processing is, or is likely to, cause you or someone else to suffer substantial damage or distress which is not justified, you can ask the data controller to stop that processing.

In any case for information or advice on your rights you can contact the Data Protection Commissioner in Jersey.

Appendix 5

SCHEDULE 4

(Article 4(3) and Schedule 1 Part 2, paragraph 14)

TRANSFERS TO WHICH EIGHTH PRINCIPLE DOES NOT APPLY

1 Consent

The data subject has consented to the transfer.

2 Contract between data subject and data controller

The transfer is necessary for –

(a) the performance of a contract between the data subject and the data controller; or

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

3 Third-party contract in interest of data subject

The transfer is necessary for –

(a) the conclusion of a contract between the data controller and a person other than the data subject, being a contract that is entered into at the request of the data subject, or is in the interests of the data subject; or

(b) the performance of such a contract.

4 Public interest

The transfer is necessary for reasons of substantial public interest.

5 Legal proceedings etc.

The transfer –

(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.

6 Vital interests

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

7 Public register

The transfer is of part of the personal data on a public register and any conditions subject to which the register is open to inspection are complied with by any person to whom the data are or may be disclosed after the transfer.

8 Transfer made on terms generally approved by Commissioner

The transfer is made on terms of a kind approved by the Commissioner as ensuring adequate safeguards for the rights and freedoms of data subjects.

9 Commissioner has authorized transfer

The transfer has been authorized by the Commissioner as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects.

10 Regulations specify what is or is not public interest

The States may by Regulations specify –

(a) circumstances in which a transfer is to be taken for the purposes paragraph 4 to be necessary for reasons of substantial public interest; and

(b) circumstances in which a transfer not required by or under an enactment is not to be taken for the purposes of paragraph 4 to be necessary for reasons of substantial public interest.