



THE OFFICE OF THE
**DATA PROTECTION
COMMISSIONER**

Data Protection (Bailiwick of Guernsey) Law, 2001 :
Code of Practice & Guidance
on the Processing of Personal Data for Credit Purposes
For data controllers based in the Bailiwick of Guernsey

Table of Contents

Introduction	2
Data Protection Principles 1 – 2	3
Data Protection Principles 3 – 4	4
Data Protection Principles 5 – 6	5
Data Protection Principles 7 – 8	6
Appendix 1 – Schedule 2	7
Appendix 2 – Schedule 3	9
Appendix 3 – Interpretation of Data Protection Principles	12
Appendix 4 – Data Protection (Credit Reference Agency) (Statement of Rights) Regulations, 2002	15
Appendix 5 – Schedule 4	20

Introduction

This Code of Practice ('the Code') has been prepared by the Data Protection Commissioner ('the Commissioner') in accordance with the powers contained within Section 51(3) of the Data Protection (Bailiwick of Guernsey) Law, 2001 ('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 ways other 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 its operation, changes in technology, industry practice or the expectations of the data subject.

Scope

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

Definitions

Unless otherwise stated, the definitions of the Data Protection (Bailiwick of Guernsey) Law, 2001 apply.

1st Data Protection Principle

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

- (a) at least one of the conditions in Schedule 2 (see Appendix 1) is met: and*
- (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 (see Appendix 2) is also met.*

Schedule 1, Part 2 of the Law provides interpretation of this principle – see 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.

Where a judgement is made in the Petty Debts Court, judgement 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 judgements that have been taken against individuals may be retained for the 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 judgement that has been set aside / abandoned should be removed from the systems of the data controller immediately any such action is publically 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 the 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 reference / debt collection agency and the organisations that have communicated 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 60 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 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) (Statement of Rights) Regulations, 2002 (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). Section 12 of the Law applies in this respect.

7th Data Protection Principle

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

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 fireproof, lockable cabinets.

Access to 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 Bailiwick 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.

No personal data should be transferred outside of the Bailiwick of Guernsey 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

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

1. The data subject has given his consent to the processing.
2. The processing is necessary –
 - (a) for the performance of a contract to which the data subject is a party, or
 - (b) for the taking of steps at the request of the data subject with a view to entering into a contract.
3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
4. The processing is necessary in order to protect the vital interests of the data subject.
5. The processing is necessary –
 - (a) for the administration of justice,
 - (b) for the exercise of any functions conferred on any person by or under any enactment,
 - (c) for the exercise of any functions of the Crown, a Law Officer of the Crown [, a department of the States or a committee of the States of Alderney or the Chief Pleas of Sark], or
 - (d) for the exercise of any other functions of a public nature exercised in the public interest by any person.
6. (1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

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

SCHEDULE 3

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

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

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

(2) The Committee may by Order –
 - (a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
 - (b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

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

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

- (ii) exists for political, philosophical, religious or trade-union purposes,
- (b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,
- (c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and
- (d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

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

6. The processing –

- (a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
- (b) is necessary for the purpose of obtaining legal advice, or
- (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7. (1) The processing is necessary –

- (a) for the administration of justice,
- (b) for the exercise of any functions conferred on any person by or under an enactment, or
- (c) for the exercise of any functions of the Crown, a Law Officer of the Crown [, a department of the States or a committee of the States of Alderney or the Chief Pleas of Sark].

(2) The Committee may by Order –

- (a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
- (b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such

further conditions as may be specified in the order are also satisfied.

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

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

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

9. (1) The processing –

- (a) is of sensitive personal data consisting of information as to racial or ethnic origin,
- (b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and
- (c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

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

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

SCHEDULE 1

PART II

INTERPRETATION OF THE PRINCIPLES IN PART I

The first principle

1. (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 authorised 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 the States.

2. (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, the information specified in sub-paragraph (3), and
- (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, the information specified in sub-paragraph (3).

(2) In sub-paragraph (1)(b) "the relevant time" means –

- (a) the time when the data controller first processes the data, or
- (b) in a case where at that time disclosure to a third party within a reasonable period is envisaged –

- (i) if the data are in fact disclosed to such a person within that 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) The information referred to in sub-paragraph (1) is as follows, namely–

- (a) the identity of the data controller,
- (b) if he has nominated a representative for the purposes of this Law, the identity of that representative
- (c) the purpose or purposes for which the data are intended to be processed, and
- (d) any further information which 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. (1) Paragraph 2(1)(b) does not apply where either of the primary conditions in sub-paragraph (2), together with such further conditions as may be prescribed by the Committee by Order, are met.

(2) The primary conditions referred to in sub-paragraph (1) are –

- (a) that the provision of that information would involve a disproportionate effort, or
- (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. (1) Personal data which contain a general identifier falling within a description prescribed by the Committee by Order 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 sub-paragraph (1) "a general identifier" means any identifier (such as, for example, a number or code used for identification purposes) which –

- (a) relates to an individual, and
- (b) forms part of a set of similar identifiers which is of general application.

The Data Protection (Credit Reference Agency) (Statement of Rights) Regulations, 2002

*Made
Coming into operation
Laid before the States*

*9th July, 2002
1st August, 2002
25th September, 2002*

THE STATES ADVISORY AND FINANCE COMMITTEE, in exercise of the powers conferred on it by sections 9(3) and 66(2) of the Data Protection (Bailiwick of Guernsey) Law, 2001^a and all other powers enabling it, and after consultation with the Data Protection Commissioner in accordance with section 66(3) of that Law, hereby makes the following Regulations -

Statement of rights under section 9(3).

1. The form in the Schedule to these Regulations, completed in accordance with the footnotes, is prescribed for the purposes of section 9(3) of the Law.

Interpretation.

2. (1) In these Regulations, unless the context otherwise requires "**the Law**" means the Data Protection (Bailiwick of Guernsey) Law, 2001.

(2) The provisions of the Interpretation (Guernsey) Law, 1948^b apply to the interpretation of these Regulations -

(a) throughout the Bailiwick; and

(b) as they apply to the interpretation of an enactment.

(3) Unless the context otherwise requires, references in these Regulations to an enactment are references thereto as amended, re-enacted (with or without modification), extended or applied.

Citation.

3. These Regulations may be cited as the Data Protection (Credit Reference Agency) (Statement of Rights) Regulations, 2002.

^a Order in Council No. V of 2002.

^b Ordres en Conseil Vol. XIII, p. 355.

Commencement.

4. These Regulations shall come into force on the 1st August, 2002.

Dated this 9th day of July, 2002.

.....

L. C. MORGAN
President of the States Advisory and Finance Committee
For and on behalf of the Committee.

SCHEDULE

CREDIT REFERENCE AGENCY FILES

INDIVIDUALS

YOUR RIGHTS UNDER THE DATA PROTECTION (BAILIWICK OF GUERNSEY)
LAW, 2001, IF YOU THINK ANY ENTRY IN OUR FILE IS WRONG

This statement of your rights is provided by [**Note 1**] together with all the information we hold about you on our files. Our postal address is [**Note 2**]

Your rights are as follows -

If you think that any of the information we have sent you is wrong and that you are likely to suffer because it is wrong, you can ask us to correct it or remove it from our file.

You need to write to us telling us what you want us to do. You should explain why you think the information is wrong.

If you write to us, we have to reply in writing within 28 days.

Our reply will tell you whether we have corrected the information, removed it from our file or done nothing. If we tell you that we have corrected the information, you will get a copy.

If our reply says that we have done nothing, or if we fail to reply within 28 days, or if we correct the information but you are not happy with the correction, you can write your own note of correction and ask for it to be included on our file.

To do this, you will need to write to us within 28 days of receiving our reply. If you did not get a reply from us and you want the information we sent you to be corrected, you will need to write to us within 8 weeks of the letter you wrote to us in which you asked us to correct the information or remove it from our file.

Your letter will need to -

- include the note of correction you have written. It must not be more than

Note 1 : Insert the name of the credit reference agency issuing the statement.

Note 2 : Insert the credit reference agency's postal address.

200 words long and should give a clear and accurate explanation of why you think the information is wrong. If the information is factually correct but you think it creates a misleading impression, your note of correction can explain why.

- ask us to add your note of correction to our file and to include a copy of it whenever we give anyone any of the information you think is wrong or any information based on it.

If we accept your note of correction, we have to tell you in writing within 28 days that we are going to add it to our file.

If we think it would be wrong to add your note of correction to our file, we have to apply for a ruling from the Data Protection Commissioner.

We will apply for a ruling if we do not want to include your note of correction because we think it is wrong, or because we think it is defamatory, frivolous or scandalous, or unsuitable for publication for some other reason. We can only refuse to include your note of correction if the Commissioner agrees with us.

If we have not written to you within 28 days of receiving your note of correction, or if we have written telling you that we are not going to add your note of correction to our file, you can appeal to the Data Protection Commissioner.

If you want to do this, you will have to write to the following address [**Note 3**]-

The Data Protection Commissioner,
Frances House,
Sir William Place,
Saint Peter Port,
Guernsey
GY1 1GX

Telephone no. 01481-742074
Fax no. 01481-742077
e.mail: dataprotection@gov.gg

When you write, you must give the following details -

- your full name and address
- our name and address
- details of the information you think is wrong, including -

Note 3 : If the address, telephone number, fax number or e.mail address of the Data Protection Commissioner have changed, substitute the correct details.

why you think it is wrong,

why you think you are likely to suffer because it is wrong, and

an indication of when you sent us your note of correction.

It would be helpful to the Commissioner if you could include a copy of your note of correction.

Before deciding what to do, the Commissioner may ask us for our side of the story and send us a copy of your letter. In return, you will be sent any comments we make.

The Commissioner can make any order he thinks fit when he has considered your appeal. For example, he can order us to accept your note of correction and add it to our file.

If at any stage we fail to correct or remove wrong information, you can ask the Data Protection Commissioner to check whether we are meeting the requirements of the Data Protection (Bailiwick of Guernsey) Law 2001.

The Data Protection (Bailiwick of Guernsey) Law 2001 requires us to take reasonable steps to check the accuracy of personal information. If you think we have failed to correct or remove wrong information about you, you have the right to ask the Data Protection Commissioner, at the above address, to check whether our dealing with your information has met this requirement.

Important Note: The various time limits referred to in this statement (mostly 28 days) start with the day following receipt and end with the day of delivery. That means (for example) that if you have 28 days to reply to a letter from us, the period starts with the day after you receive our letter; and you then have to make sure that your reply is delivered to us no later than 28 days from that date. In order to avoid the risk of losing your rights you should therefore allow for postal delays.

**SCHEDULE 4
CASES WHERE THE EIGHTH PRINCIPLE DOES NOT APPLY**

1. The data subject has given his consent to the transfer.
2. The transfer is necessary-
 - (a) for the performance of a contract between the data subject and the data controller; or
 - (b) for the taking of steps at the request of the data subject with a view to his entering into a contract with the data controller.
3. The transfer is necessary-
 - (a) for the conclusion of a contract between the data controller and a person other than the data subject which-
 - (i) is entered into at the request of the data subject; or
 - (ii) is in the interests of the data subject; or
 - (b) for the performance of such a contract.
4. (1) The transfer is necessary for reasons of substantial public interest.
(2) The Committee may by Order specify-
 - (a) circumstances in which a transfer is to be taken for the purposes of sub-paragraph (1) to be necessary for reasons of substantial public interest; and
 - (b) circumstances in which a transfer which is not required by or under an enactment is not to be taken for the purpose of sub-paragraph (1) to be necessary for reasons of substantial public interest.
5. The transfer-
 - (a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings);

- (b) is necessary for the purpose of obtaining legal advice; or
- (c) necessary for the purposes of establishing, exercising or defending legal rights.

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

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

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