# Accessing Communications Data

## Code of Practice

### Regulation of Investigatory Powers (Bailiwick of Guernsey) Law, 2003

# Accessing Communications Data

## Code of Practice

*(Made pursuant to Section 61 of the Regulation of Investigatory Powers (Bailiwick of Guernsey) Law, 2003)*

CONTENTS

## INTRODUCTION

**1.1** This Code of Practice relates to the powers and duties conferred or imposed under Chapter II of Part I of the Regulation of Investigatory Powers (Bailiwick of Guernsey) Law 2003 ("the Law"). It provides guidance on the procedures that must be followed before access to communications data can take place under those provisions.

**1.2** The Code should be readily available to any members of a public authority who are involved in operations to access communications data.

**1.3** The Law provides that the Code is admissible in evidence in criminal and civil proceedings. If any provision of the Code appears relevant to a question before any court or tribunal hearing any such proceedings, or to the Tribunal established under the Law, or to the Commissioner responsible for overseeing the powers conferred by the Law, it must be taken into account.

**1.4** This Code applies to relevant public authorities as described in Chapter II of Part I of the Law [*see paragraph 3.1 below*], and extends throughout the Bailiwick.

**1.5** This Code does not cover conduct consisting in the interception of communications (contents of a communication).

## GENERAL

**2.1** The Code covers any conduct in relation to a postal service or telecommunication system for obtaining communications data and the disclosure to any person of such data. For these purposes, communications data includes information relating to the use of a postal service or telecommunication system but does not include the contents of the communication itself, contents of e-mails or interactions with websites. In this

Code "data", in relation to a postal item, means anything written on the outside of the item.

**2.2** A person who engages in such conduct must be properly authorised and must act in accordance with that authority.

**2.3** A test of necessity [*see paragraphs 4.1- 4.3*] must be met before any communications data is obtained. The assessment of necessity is one made by a designated person. (This is a person designated for the purposes of Chapter II of Part I of the Law (see Para 3.2 below). A designated person has a number of obligations within the provisions of the Law, which must be met before communications data is obtained. These are also laid out in this Code). A designated person must not only consider it necessary to obtain the communications data but must also consider that the conduct involved in obtaining the communications data will be proportionate [*see paragraph 4.4 below*] to what it is sought to achieve.

## DESIGNATED PERSONS PERMITTED TO ACCESS COMMUNICATIONS DATA

**3.1** Only designated persons within a "relevant public authority" are permitted under the Law to grant authorisations or serve notices, the two routes by which the Law allows communications data to be accessed [*see further paragraph 5.1 below*]. The persons designated under the Law, and the relevant public authority for which they can act are –

- the Chief Officer of the Island Police Force (for the Island Police Force)
- the Chief Officer of Customs and Excise (for Customs and Excise)
- Her Majesty's Procureur (for any of the Intelligence Services or any other public authority within the Bailiwick).

**3.2** The Law permits the Home Affairs Committee to provide in regulations for the designated person to authorise individuals holding such offices, ranks or positions with the same public authority to act on his behalf in granting authorisations or notices for access to communications data. The Committee may also by regulation place restrictions on:

- the authorisations or notices that may be granted or given by designated persons; and

- the circumstances in which, or purposes for which, authorisations or notices may be granted or given.

**3.3** The Regulations made by the Committee[1] allow for the following appropriate level of official within each public authority to grant authorisations or give notices:

- For the Island Police Force,

    - an officer of not less than Chief Inspector may authorise Line/Advanced Data (Itemised Billing, etc)

    - an officer of not less than Inspector may authorise Personal Data (subscriber checks)

- For the Customs and Excise,

---

1 The Regulation of Investigatory Powers (Bailiwick of Guernsey) (Prescription of Offices, Ranks and Positions) Regulations, 2004.

- an officer of not less than Surveyor may authorise Line/Advanced Data (Itemised Billing, etc)

- an officer of not less than Senior Investigating Officer may authorise Personal Data (subscriber checks)

## PURPOSES FOR WHICH COMMUNICATIONS DATA MAY BE SOUGHT

**4.1** Under section 18(2) of the Law, communications data may be sought if a designated person believes it is necessary for one or more of the following purposes:

- in the interests of national security;

- for the purpose of preventing or detecting crime or of preventing disorder;

- in the interests of the economic well-being of the Bailiwick [*see paragraph 4.2*];

- in the interests of public safety;

- for the purpose of protecting public health;

- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;

- for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health.[2]

**4.2** In exercising the power to grant an authorisation or give a notice in the interests of the economic well-being of the Bailiwick (as provided for by section 18(2)of the Law), a designated person will consider whether the economic well-being of the Bailiwick which it is in the interests of, is, on the facts of each case, related to national security. A designated person will not grant an authorisation or give a notice on section 18(2)(c) grounds if this link is not established. An application for an authorisation or a notice on section 18(2)(c) grounds should therefore explain how, in the applicant's view, the interests of the economic well-being of the Bailiwick are related to national security on the facts of the case.

**4.3** For an action to be necessary in a democratic society the access to communications data must pursue one of the legitimate aims listed in paragraph 4.1, and must also fulfil a pressing social need and be an action proportionate to that aim.

**4.4** Under section 18(5) of the Law, a designated person must also consider that the conduct involved in obtaining the communications data will be proportionate. Proportionality is a crucial concept. In both the Law and this Code, reference is made to the conduct being proportionate. This means that even if an action in a particular instance (which interferes with a Convention right) is directed at pursuing a legitimate aim (as listed in paragraph 4.1), this will not justify the interference if the means used to achieve the aim are excessive in the circumstances. Any interference with a Convention right

---

2 The Law allows the Home Affairs Committee to add further purposes to this list by means of Regulations.

should be carefully designed to meet the objective in question and must not be arbitrary or unfair. Even taking all these considerations into account, in a particular case interference may still not be justified because the impact on the individual or group is too severe.

## AUTHORISATIONS AND NOTICES

**5.1** The Law provides two different ways of authorising access to communications data; through an authorisation under section 18(3) and, more usually, by a notice under section 18(4). An authorisation would allow the relevant public authority to collect or retrieve the data itself. A notice is given to a postal or telecommunications operator and requires that operator to collect or retrieve the data and provide it to the public authority, which served the notice. The designated person decides whether or not an authorisation should be granted or a notice given.

**5.2** In order to illustrate, a section 18(3) authorisation may be appropriate where:

- the postal or telecommunications operator is not capable of collecting or retrieving the communications data; [3]

- it is believed the investigation may be prejudiced if the postal or telecommunications operator is asked to collect the data itself;

- there is a prior agreement in place between the relevant public authority and the postal or telecommunications operator as to the appropriate mechanisms for the disclosure of communications data.

---

[3] Where possible, this assessment will be based upon information provided by the relevant postal or telecommunications operator.

5.3 Applications for access to communications data should only be made by persons in the same public authority as a designated person.

**(a) Single points of contact within relevant public authorities**

5.4 Notices (and where appropriate, authorisations) for communications data should be channelled through a single point of contact within each public authority (unless the exemptions in paragraphs 5.13 - 5.14 applies). This will provide for an efficient regime, since the single points of contact will deal with the postal or telecommunications operator on a regular basis. It will also help the public authority to regulate itself. This will assist in reducing the burden on the postal or telecommunications operator by such requests. Single points of contact will be able to advise a designated person on whether an authorisation or a notice is appropriate.

5.5 The single point of contact should be in a position to:

- where appropriate, assess whether access to communications data is reasonably practical for the postal or telecommunications operator;

- advise applicants and designated persons on the practicalities of accessing different types of communications data from different postal or telecommunications operators;

- provide safeguards for authentication.

**(b) Applications to obtain communications data under the Law**

5.6 The application form is subject to inspection by the Commissioner and both applicant and designated person may be required to justify their decisions. Applications to obtain communications data under the Law should be made on a standard form (paper or electronic), which must be retained by the public

authority (see section 7 of this Code) and which should contain the following minimum information:

- the name (or designation) of the officer requesting the communications data;

- the operation and person (if known) to which the requested data relates;

- a description, in as much detail as possible, of the communications data requested (the application should also identify what type of data is sought i.e., whether it falls within paragraph (a), (b) or (c) of the definition of communications data in section 67(3) of the Law);

- the reason why obtaining the requested data is considered to be necessary for one or more of the purposes in paragraph 4.1 above (the relevant purpose also needs to be identified);

- an explanation of why obtaining the data constitutes conduct proportionate to what it seeks to achieve;

- where appropriate, consideration of any collateral intrusion, the extent to which the privacy of others may be affected and why that intrusion is justified; and

- the timescale within which the communications data is required. Where the timescale within which the material is required is any greater than usual, the reasoning for this should also be included.

**5.7** The application form should subsequently record whether access to communications data was approved or denied, by whom and the date.

Alternatively, the application form can be marked with a cross-reference to the relevant authorisation or notice.

**(c) Considerations for designated person**

**5.8** The designated person must take account of the following points, in order to be sure that his decision is properly informed and so that he is able to justify the decisions made:

- whether the circumstances justify the accessing of communications data for one or more of the purposes listed in paragraph 4.1 of this Code, and why obtaining the data is **necessary** for that purpose;

- whether obtaining access to the data by the conduct authorised by the authorisation, or required of the postal or telecommunications operator in the case of a notice, is **proportionate** to what is sought to be achieved. (A designated person needs to have in mind the conduct, which he is authorising or requiring in each case. In making a judgement as to proportionality, a designated person needs to have in mind whether he is granting an authorisation or issuing a notice, and also what the scope of the conduct is. For example, where the conduct covers the provision of ongoing communications data);

- where appropriate, where accessing the communications data is likely to result in collateral intrusion, whether the circumstances of the case still justify that access; and whether any urgent timescale is justified.

**(d) Content of an authorisation**

**5.9** An authorisation itself can only authorise conduct to which Chapter II of Part I of the Law applies. The designated person will make a decision whether to grant an authorisation based upon the details given in the application. The application form and the authorisation itself are not served upon the holder of

communications data. The authorisation should be in a standard format (written or electronic), and should also contain a unique reference number. The authorisation, a copy of which must be retained by the public authority (see section 7 of this Code), must contain the following information:

- a description of the conduct to which Chapter II of Part I of the Law applies that is authorised;
- a description of the required communications data;
- for which of the purposes in paragraph 4.1 above the data is required;
- and the name (or designation) and office, rank or position of the designated person.

**(e) Content of a notice**

**5.11** A designated person will make a decision whether to issue a notice based upon the application, which is made. The application form is not served upon the holder of communications data. The notice that they receive contains only enough information to allow them to fulfil their duties under the Law. The notice served upon the holder of the communications data should be in a standard format (written or electronic), a copy of which must be retained by the public authority (see section 7 of this Code), and which must contain the following information:

- a description of the required communications data;
- for which of the purposes set out in paragraph 4.1 of this Code the data is required;

- the name (or designation) and office, rank or position of the designated person;

- the manner in which the data should be disclosed.

**5.12** The notice should also contain:

- a unique reference number;

- where appropriate, an indication of any urgency for response;

- a statement stating that data is sought under the provisions of Chapter II of Part I of the Law. i.e. an explanation that compliance with this notice is a legal requirement; and

- contact details so that the veracity of the notice may be checked.

A specimen copy of a notice can be found at Annex A to this Code.

**(f) Oral authority (urgent cases)**

**5.13** An application for communications data may only be made and approved orally, on an urgent basis, where it is necessary to obtain communications data for the purpose set out in section 18(2)(g) of the Law[4] i.e.:

*"for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health".*

---

[4] In order to give effect to Article 2 of the European Convention on Human Rights (the right to life).

**5.14** The fact of an oral application and approval must be recorded by the applicant and designated person at the time or as soon as possible afterwards. In these circumstances, an authorisation under section 18(3) of the Law must be completed (in a written or electronic format) as soon as practicable thereafter. In the case of a notice under section 18(4) of the Law, a designated person may make an oral request to a postal or telecommunications operator to disclose communications data urgently, which must be followed by a (written or electronic) notice to the postal or telecommunications operator very shortly thereafter. In these urgent situations, a section 18(4) notice may be issued directly to the postal or telecommunications operator, therefore relaxing the need to do so via a single point of contact.

**(g) Disclosure of data**

**5.15** Notices under section 18(4) of the Law will only require the disclosure of data to:

- the person giving the notice i.e. the designated person; or

- to another specified person who must be from the same relevant public authority. In practice, this is likely to be the single points of contact.

**5.16** The notice issued under section 18(4) may require the recipient of the notice, and others who become aware of the existence or the contents of the notice, to keep secret anything to do with the matter. This obligation applies equally to disclosure within the law enforcement agency and any other public authority concerned. The public authority and the postal or telecommunications operator should ensure that safeguards are in place to limit disclosure, copying and distribution of the notice to the minimum necessary to achieve successful compliance. The notice and any copies of it should be kept securely, together with any information or data obtained as a result of the notice. When no longer required, and upon expiry or cancellation, the notice and any copies

should be returned by the postal or telecommunication operator to the public authority issuing the notice.

**5.17** A person who discloses information in breach of the obligation to keep secret anything to do with a notice may commit an offence under section 18(10) of the Law, which is punishable with a maximum of five years imprisonment or a fine or both. It would be a defence if the person can show that he could not reasonably be expected to prevent disclosure in the circumstances, or where the disclosure takes place to an Advocate or other professional legal advisor in connection with obtaining legal advice. It would also be a defence if the disclosure was made or authorised by the Commissioner.

## VALIDITY OF AUTHORISATIONS AND NOTICES

### (a) Duration

**6.1** Authorisations and notices will only be valid for one month. This period will begin when the authorisation is granted or the notice given. A designated person should specify a shorter period if that is satisfied by the request, since this may go to the proportionality requirements. For 'future' communications data disclosure may only be required of data obtained by the postal or telecommunications operator within this period i.e. up to one month. For 'historical' communications data, disclosure may only be required of data in the possession of the postal or telecommunications operator. A postal or telecommunications operator should comply with a section 18(4) notice as soon as is reasonably practicable. Furthermore, they will not be required to supply data unless it is reasonably practicable to do so.

### (b) Renewal

**6.2** An authorisation or notice may be renewed at any time during the month it is valid, by following the same procedure as in obtaining a fresh authorisation or notice.

**6.3** A renewed authorisation or notice takes effect at the point at which the authorisation or notice it is renewing expires.

**(c) Cancellation**

**6.4** A designated person shall cancel a notice given under section 18(4) of the Law as soon as it is no longer necessary, or the conduct is no longer proportionate to what is sought to be achieved. The duty to cancel a notice falls on the designated person who issued it.

**6.5** As a matter of good practice, authorisations should also be cancelled in accordance with the procedure above.

**6.6** In the case of a section 18(4) notice, the relevant postal or telecommunications operator will be informed of the cancellation.

**6.7** The Law permits regulations to be made under section 19(9) prescribing the appropriate level of official within each public authority who may cancel a notice in the event of the designated person no longer being able to perform this duty.

## RETENTION OF RECORDS BY PUBLIC AUTHORITIES

**7.1** Applications, authorisations and notices for communications data must be retained by the relevant public authority until it has been audited by the Commissioner. The public authority should also keep a record of the dates on which the authorisation or notice is started and cancelled.

**7.2** Applications must also be retained to allow for the complaints Tribunal, under Part IV of the Law, to carry out its functions.

**7.3** This Code does not affect any other obligations placed on public authorities to retain data, whether under any enactment, or by reason of customary or

common law. For example, relevant material gathered in the course of a criminal investigation may require retention so as to ensure the fairness of a trial.

**(a) Errors**

**7.4** Where any errors have occurred in the granting of authorisations or the giving of notices, a record should be kept, and a report and explanation sent to the Commissioner as appropriate.

**(b) Data protection safeguards**

**7.5** Communications data, and all copies, extracts and summaries of it, must be handled and stored securely. In addition, the requirements of the Data Protection (Bailiwick of Guernsey) Law 2001 and its data protection principles should be adhered to[5].

## SCRUTINY

**8.1** The Law provides for a Commissioner whose remit is to provide independent scrutiny of the use of the powers contained within Part I.

**8.2** This Code does not cover the exercise of the Commissioner's functions. However, it will be the duty of any person who uses the powers conferred by Chapter II of Part I to comply with any request made by the Commissioner to provide any information he requires for the purposes of enabling him to discharge his functions.

---

5 Further guidance is available from http://www.dpcommission.gov.gg/

## COMPLAINTS

**9.1** The Law establishes an independent Tribunal, which is made up of senior members of the legal profession or judiciary and is independent of the States of Deliberation or any Committee or public administrative body in the Bailiwick. The Tribunal has full powers to investigate and decide any case within its jurisdiction.

**9.2** This Code does not cover the exercise of the Tribunal's functions. However, details of the relevant complaints procedure should be readily available, for reference purposes, at the police station and at customs offices, or can be obtained from the following address:

The Secretary to the Tribunal,
Investigatory Powers Tribunal
PO Box 82,
Guernsey GY1 4BR.

**ANNEX A**

| REF NUMBER: |
| --- |
| |

# RESTRICTED

**Notice under section 18(4) of the Regulation of Investigatory Powers (Bailiwick of Guernsey) Law, 2003 requiring communications data to be obtained and disclosed.**

** Omit as appropriate*

**TO**: *(Name of postal or telecommunications operator and address)*

In accordance with section 18(4) of the Regulation of Investigatory Powers (Bailiwick of Guernsey) Law 2003, I hereby require you –

*(a) if not already in possession of the data to which this notice relates, to obtain it; and

*[for use in those cases where you are actually asking for data to be captured for the duration of the notice – this paragraph should be omitted where you are only requiring the disclosure of historical data].*

(b) to disclose all communications data to which this notice relates, whether in your possession or subsequently obtained by you.

**Description of communications data to which this notice relates:**

*[enter here details of the communications data required. Distinguish here between data (a) to be obtained if not already in the possession of the operator - omit if not relevant- and (b) to be disclosed - each should be described separately].*

*(a) [*communications data to be obtained*];

(b) [*communications data to be disclosed*].

**This notice is valid from**:

*[start date – issue date of this notice - to (end date). – End date must be no more than one month from the date of this notice, or earlier if cancelled under section 19(8)).*

This notice may be renewed at any time before the end of the period of one month starting with [*issue date*] by the giving of a further notice.

I believe that it is necessary for this communications data to be obtained for the following purpose(s):

*[List the purpose(s) that the communications data is required for (from Section 18(2)) - follow the statutory language exactly)].*

In reaching this conclusion I have satisfied myself that obtaining this data by the conduct required by this notice is proportionate to what is sought to be achieved by so obtaining the data.

**You are required to produce the said communications data to:**

*[specify the person to whom the data is to be disclosed – the name and office, rank or position must be specified]*
of *[public authority]*
for him to take away as specified below:

[*Specify the manner in which the data is to be disclosed*].

Date .....

**Designated Person**: [*Enter name, and office, rank or position, and signature*]

This notice may be verified by contacting the following person:
[*enter contact details i.e. of the Single Point of Contact*]

***TAKE NOTE that you are required to keep secret the fact that this notice has been given, the contents of it, and anything which is done in pursuance of it. Unauthorised disclosure is a criminal offence, punishable with up to five years imprisonment, or a fine, or both.**