Jersey

REGULATION OF INVESTIGATORY POWERS (CODES OF PRACTICE) (JERSEY) ORDER 2006

Arrangement

Article

Jersey

REGULATION OF INVESTIGATORY POWERS (CODES OF PRACTICE) (JERSEY) ORDER 2006

Made *6th December 2006*

Coming into force *in accordance with Article 6*

THE MINISTER FOR HOME AFFAIRS, in pursuance of Article 51 of the Regulation of Investigatory Powers (Jersey) Law 2005[1], orders as follows –

1 Code of practice on interception of communications

The code of practice on the interception of communications set out in Schedule 1 shall have effect.

2 Code of practice on interception of communications – postal

The code of practice on the interception of communications set out in Schedule 2 shall have effect.

3 Code of practice on accessing communications data

The code of practice on accessing communications data set out in Schedule 3 shall have effect.

4 Code of practice on covert surveillance

The code of practice on covert surveillance set out in Schedule 4 shall have effect.

5 Code of practice on covert human intelligence sources

The code of practice on covert human intelligence sources set out in Schedule 5 shall have effect.

6 Citation and commencement

This Order may be cited as the Regulation of Investigatory Powers (Codes of Practice) (Jersey) Order 2006 and shall come into force on the same day as the Regulation of Investigatory Powers (Jersey) Law 2005.

SENATOR W. KINNARD

Minister for Home Affairs

SCHEDULE 1

(Article 1)

CODE OF PRACTICE ON INTERCEPTION OF COMMUNICATIONS

CONTENTS

1 GENERAL

1.1 This code of practice relates to the powers and duties conferred or imposed under Chapter 1 of Part 1 of the Regulation of Investigatory Powers (Jersey) Law 2005 (the "Law"). It provides guidance on the procedures that must be followed before interception of communications can take place under those provisions. It is primarily intended for use by those public authorities listed in Article 11 of the Law. It will also prove useful to postal and telecommunication operators and other interested bodies to acquaint themselves with the procedures to be followed by those public authorities.

1.2 The Law provides that all codes of practice relating to the Law are admissible as evidence in criminal and civil proceedings. If any provision of this code appears relevant before any court or tribunal considering 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.

2 GENERAL RULES ON INTERCEPTION WITH A WARRANT

2.1 There are a limited number of persons by whom, or on behalf of whom, applications for interception warrants may be made. These persons are:

- Chief Officer, States of Jersey Police;
- Agent of the Impôts;
- Chief Inspector of Immigration;
- Director-General of the Security Services;
- Chief of the Secret Intelligence Services;
- Director of GCHQ;
- Chief of the Defence Intelligence Services;
- A person who, for the purposes of any international mutual assistance agreement, is the competent authority of a country or territory outside Jersey.

2.2 All interception warrants are issued by the Attorney General.

2.3 Before issuing an interception warrant, the Attorney General must believe that what the action seeks to achieve is necessary for one of the following Article 10(3) purposes:

- in the interests of national security;
- for the purpose of preventing or detecting serious crime;
- for the purpose of safeguarding the economic well-being of Jersey; or
- for the purpose of giving effect to any international mutual assistance treaty;

and that the conduct authorized by the warrant is proportionate to what is sought to be achieved by that conduct.

Necessity and Proportionality

2.4 Obtaining a warrant under the Law will only ensure that the interception authorized is a justifiable interference with an individual's rights under Article 8 of the European Convention of Human Rights (the right to privacy) if it is necessary and proportionate for the interception to take place. The Law recognises this by first requiring that the Attorney General believes that the authorization is necessary on one or more of the statutory grounds set out in Article 10(3) of the Law. This requires the Attorney General to believe that it is necessary to undertake the interception which is to be authorized for a particular purpose falling within the relevant statutory ground.

2.5 Then, if the interception is necessary, the Attorney General must also believe that it is proportionate to what is sought to be achieved by carrying it out. This involves balancing the intrusiveness of the interference, against the need for it in operational terms. Interception of

communications will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other means. Further, all interception should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

Implementation of Warrants

2.6 After a warrant has been issued it will be forwarded to the person to whom it is addressed, in practice the intercepting agency which submitted the application. The Law (Article 15) then permits the intercepting agency to carry out the interception, or to require the assistance of other persons in giving effect to the warrant. Warrants cannot be served on those outside Jersey.

Provision of Reasonable Assistance

2.7 Any postal or telecommunications operator (referred to as communications service providers) in Jersey may be required to provide assistance in giving effect to an interception. The Law places a requirement on postal and telecommunications operators to take all such steps for giving effect to the warrant as are notified to them (Article 15(4) of the Law). But the steps which may be required are limited to those which it is reasonably practicable to take (Article 15(5)). What is reasonably practicable should be agreed after consultation between the postal or telecommunications operator and the Attorney General. If no agreement can be reached it will be for the Attorney General to decide whether to press forward with civil proceedings or whether criminal proceedings may also be instituted.

2.8 Where the intercepting agency requires the assistance of a communications service provider in order to implement a warrant, they should provide the following to the communications service provider:

- A copy of the warrant instrument signed and dated by the Attorney General;
- The relevant schedule for that service provider setting out the numbers, addresses or other factors identifying the communications to be intercepted;
- A covering document from the intercepting agency requiring the assistance of the communications service provider and specifying any other details regarding the means of interception and delivery as may be necessary. Contact details with respect to the intercepting agency will either be provided in this covering document or will be available in the handbook provided to all postal and telecommunications operators who maintain an intercept capability.

Provision of Intercept Capability

2.9 Whilst all persons who provide a postal or telecommunications service are obliged to provide assistance in giving effect to an interception, persons who provide a public postal or telecommunications service, or plan to do so, may also be required to provide a reasonable intercept capability (Article 16). The obligations the Minister for Home Affairs

considers reasonable to impose on such persons to ensure they have such a capability will be set out in an order made by the Minister. The Minister may then serve a notice upon a communications service provider setting out the steps they must take to ensure they can meet these obligations. A notice will not be served without consultation over the content of the notice between the Minister and the service provider having previously taken place. When served with such a notice, a communications service provider, if the provider feels it unreasonable, will be able to refer that notice to the Technical Advisory Board (TAB) on the reasonableness of the technical requirements and capabilities that are being sought. Details of how to submit a notice to the TAB will be provided either before or at the time the notice is served.

2.10 Any communications service provider obliged to maintain a reasonable intercept capability may be provided with written guidance, or a handbook, which will contain the basic information the provider requires to respond to requests for reasonable assistance for the interception of communications.

Duration of Interception Warrants

2.11 All interception warrants are valid for an initial period of 3 months. Upon renewal, warrants issued on serious crime grounds are valid for a further period of 3 months. Warrants renewed on national security/economic well-being grounds are valid for a further period of 6 months.

2.12 Where a change in circumstance prior to the set expiry date leads the intercepting agency to consider it no longer necessary or practicable for the warrant to be in force, it should be cancelled with immediate effect.

Stored Communications

2.13 Article 2(6) of the Law defines a communication in the course of its transmission as also encompassing any time when the communication is being stored on the communication system in such a way as to enable the intended recipient to have access to it. This means that a warrant can be used to obtain both communications that are in the process of transmission and those that are being stored on the transmission system.

2.14 Stored communications may also be accessed by means other than a warrant. If a communication has been stored on a communication system it may be obtained with lawful authority by means of an existing statutory power such as a production order (under the Police Procedures and Criminal Evidence (Jersey) Law 2003) or a search warrant.

3 SPECIAL RULES ON INTERCEPTION WITH A WARRANT

Collateral Intrusion

3.1 Consideration should be given to any infringement of the privacy of individuals who are not the subject of the intended interception, especially where communications relating to religious, medical, journalistic or legally privileged material may be involved. An application for an interception warrant should draw attention to any circumstances which give rise to an unusual degree of collateral infringement of privacy, and this will be taken into account by the

Attorney General when considering a warrant application. Should an interception operation reach the point where individuals other than the subject of the authorization are identified a directly relevant to the operation, consideration should be given to applying for separate warrants covering those individuals.

Confidential Information

3.2 Particular consideration should also be given in cases where the subject of the interception might reasonably assume a high degree of privacy, or where confidential information is involved. Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material (see paragraphs 3.9 - 3.11). For example, extra consideration should be given where interception might involve communications between a minister of religion and an individual relating to the latter's spiritual welfare, or where matters of medical or journalistic confidentiality or legal privilege may be involved.

Communications Subject to Legal Privilege

3.3 Article 5 of the Police Procedures and Criminal Evidence (Jersey) Law 2003 describes those matters that are subject to legal privilege.

3.4 Legal privilege does not apply to communications made with the intention of furthering a criminal purpose (whether the lawyer is acting unwittingly or culpably). Legally privileged communications will lose their protection if there are grounds to believe, for example, that the professional legal advisor is intending to hold or use the information for a criminal purpose. But privilege is not lost if a professional legal advisor is properly advising a person who is suspected of having committed a criminal offence. The concept of legal privilege applies to the provision of professional legal advice by any individual, agency or organisation qualified to do so.

3.5 The Law does not provide any special protection for legally privileged communications. Nevertheless, intercepting such communications is particularly sensitive and is therefore subject to additional safeguards under this Code. The guidance set out below may in part depend on whether matters subject to legal privilege have been obtained intentionally or incidentally to some other material which has been sought.

3.6 In general, any application for a warrant which is likely to result in the interception of legally privileged communications should include, in addition to the reasons why it is considered necessary for the interception to take place, an assessment of how likely it is that communications which are subject to legal privilege will be intercepted. In addition, it should state whether the purpose (or one of the purposes) of the interception is to obtain privileged communications. This assessment will be taken into account by the Attorney General in deciding whether an interception is necessary under Article 10(3) of the Law and whether it is proportionate. In such circumstances, the Attorney General will be able to impose additional conditions such as regular reporting arrangements so as to be able to exercise his or her discretion on whether a warrant should

continue to be authorized. In those cases where communications which include legally privileged communications have been intercepted and retained, the matter should be reported to the Commissioner during the Commissioner's inspections and the material be made available to the Commissioner if requested.

3.7 Where an Advocate or Solicitor or other professional legal adviser is the subject of an interception, it is possible that a substantial proportion of the communications which will be intercepted will be between the lawyer and his or her client(s) and will be subject to legal privilege. Any case where a lawyer is the subject of an investigation should be notified to the Commissioner during the Commissioner's inspections and any material which has been retained should be made available to the Commissioner if requested.

3.8 In addition to safeguards governing the handling and retention of intercept material as provided for in Article 19 of the Law, investigators who examine intercepted communications should be alert to any intercept material which may be subject to legal privilege. Where there is doubt as to whether the communications are subject to legal privilege, advice should be sought from the Law Officers' Department. Advice should also be sought where there is doubt over whether communications are not subject to legal privilege due to the "in furtherance of a criminal purpose" exception.

Communications involving Confidential Personal Information and Confidential Journalistic Material

3.9 Similar consideration to that given to legally privileged communications must also be given to the interception of communications that involve confidential personal information and confidential journalistic material. Confidential personal information is information held in confidence concerning an individual (whether living or dead) who can be identified from it, and the material in question relates to the individual's physical or mental health or to spiritual counselling. Such information can include both oral and written communications. Such information as described above is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. For example, confidential personal information might include consultations between a health professional and a patient, or information from a patient's medical records.

3.10 Spiritual counselling is defined as conversations between an individual and a Minister of Religion acting in his or her official capacity, and where the individual being counselled is seeking or the Minister is imparting forgiveness, absolution or the resolution of conscience with the authority of the Divine Being(s) of their faith.

3.11 Confidential journalistic material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.

4 INTERCEPTION WARRANTS (ARTICLE 12(1))

4.1 This chapter applies to the interception of communications by means of a warrant complying with Article 12(1) of the Law. This type of warrant may be issued in respect of the interception of communications carried on any postal service or telecommunications system as defined in Article 2 of the Law (including a private telecommunications system). Responsibility for the issuing of interception warrants rests with the Attorney General.

Application for an Article 12(1) Warrant

4.2 An application for a warrant is made to the Attorney General. Interception warrants, when issued, are addressed to the person who submitted the application. This person may then serve a copy upon any person who may be able to provide assistance in giving effect to that warrant. Each application, a copy of which must be retained by the applicant, should contain the following information:

- Background to the operation in question.
- Person or premises to which the application relates (and how the person or premises feature in the operation).
- Description of the communications to be intercepted, details of the communications service provider(s) and an assessment of the feasibility of the interception operation where this is relevant.
- Description of the conduct to be authorized as considered necessary in order to carry out the interception, where appropriate.
- An explanation of why the interception is considered to be necessary under the provisions of Article 10(3).
- A consideration of why the conduct to be authorized by the warrant is proportionate to what is sought to be achieved by that conduct.
- A consideration of any unusual degree of collateral intrusion and why that intrusion is justified in the circumstances. In particular, where the communications in question might affect religious, medical or journalistic confidentiality or legal privilege, this must be specified in the application.
- Where an application is urgent, supporting justification should be provided.
- An assurance that all material intercepted will be handled in accordance with the safeguards required by Article 19 of the Law.

Authorization of an Article 12(1) Warrant

4.3 Before issuing a warrant under Article 12(1), the Attorney General must believe the warrant is necessary:

- in the interests of national security;
- for the purpose of preventing or detecting serious crime; or
- for the purpose of safeguarding the economic well-being of the United Kingdom.

- For the purpose of giving effect to the provisions of any international mutual assistance treaty.

4.4 In exercising the Attorney General's power to issue an interception warrant for the purpose of safeguarding the economic well-being of Jersey (as provided for by Article 10(3)(c) of the Law), the Attorney General will consider whether the economic well-being of Jersey which is to be safeguarded is, on the facts of each case, directly related to national security. The Attorney General will not issue a warrant on Article 10(3)(c) grounds if this direct link between the economic well-being of Jersey and national security is not established. Any application for a warrant on Article 10(3)(c) grounds should therefore explain how, in the applicant's view, the economic well-being of Jersey which is to be safeguarded is directly related to national security on the facts of the case.

4.5 The Attorney General must also consider that the conduct authorized by the warrant is proportionate to what it seeks to achieve (Article 10(2)(b)). In considering necessity and proportionality, the Attorney General must take into account whether the information sought could reasonably be obtained by other means (Article 10(4)).

Format of an Article 12(1) Warrant

4.6 Each warrant comprises 2 sections, a warrant instrument signed by the Attorney General listing the subject of the interception or set of premises, a copy of which each communications service provider will receive, and a schedule or set of schedules listing the communications to be intercepted. Only the schedule relevant to the communications that can be intercepted by the specified communications service provider will be provided to that service provider.

4.7 The warrant instrument should include:

- The name or description of the interception subject or of a set of premises in relation to which the interception is to take place.
- A warrant reference number.
- The persons who may subsequently modify the scheduled part of the warrant in an urgent case (if authorized in accordance Article 14(5) of the Law).

4.8 The scheduled part of the warrant will comprise one or more schedules. Each schedule should contain:

- The name of the communication service provider, or the other person who is to take action.
- A warrant reference number
- A means of identifying the communications to be intercepted.

Modification of Article 12(1) warrant

4.9 Interception warrants may be modified under the provisions of Article 14 of the Law. The unscheduled part of a warrant may only be modified by the Attorney General. The modification will expire on the expiry date of the warrant.

4.10 Scheduled parts of a warrant may be modified by the Attorney General in which case the modification expires on the expiry date of the warrant. A

modification to the scheduled part of the warrant may include the addition of a new schedule relating to a communication service provider or when a copy of the warrant has not been previously served. In an urgent case, where the warrant specifically authorizes it, scheduled parts of a warrant may be modified by the person to whom the warrant is addressed (the person who submitted the application) or a subordinate (where the subordinate is identified in the warrant). Modifications of this kind are valid for 5 working days following the day of issue unless the modification instrument is endorsed by the Attorney General. Where the modification is endorsed in this way, the modification expires upon the expiry date of the warrant.

4.11 There is a duty to modify a warrant by deleting a communications identifier if it is no longer relevant. When a modification is sought to delete a number or other communication identified, the relevant communication service provider must be advised and the interception suspended before the modification is made.

Renewal of Article 12(1) Warrant

4.12 The Attorney General may renew a warrant at any point before its expiry date. Applications for renewals must be made to the Attorney General and should contain an update of the matters outlined in paragraph 4.2 above. In particular, the applicant should give an assessment of the value of interception to the operation to date and explain why the applicant considers that interception continues to be necessary for one or more of the purposes in Article 10(3).

4.13 Where the Attorney General is satisfied that the interception continues to meet the requirements of the Law the Attorney General may renew the warrant. Where the warrant is issued on serious crime grounds, the renewed warrant is valid for a further 3 months. Where it is issued on national security/economic well-being grounds, the renewed warrant is valid for 6 months. These dates run from the date of signature on the renewal instrument.

4.14 A copy of the warrant renewal instrument will be forwarded by the intercepting agency to all relevant communications service providers on whom a copy of the original warrant instrument and a schedule have been served, providing they are still actively assisting. A warrant renewal instrument will include the reference number of the warrant and description of the person or premises described in the warrant.

Warrant Cancellation

4.15 The Attorney General is under a duty to cancel an interception warrant if, at any time before its expiry date, the Attorney General is satisfied that the warrant is no longer necessary on grounds falling within Article 10(3) of the Law. Intercepting agencies will therefore need to keep their warrants under continuous review.

4.16 The cancellation instrument should be addressed to the person to whom the warrant was issued (the intercepting agency) and should include the reference number of the warrant and the description of the person or premises specified in the warrant. A copy of the cancellation instrument

should be sent to those communications service providers who have held a copy of the warrant instrument and accompanying schedule during the preceding 12 months.

Records

4.17 The independent scrutiny régime allows the Commissioner appointed under the Law to inspect the warrant application on which the Attorney General based his or her decision and the applicant may be required to justify the content. Each intercepting agency should keep the following to be made available for scrutiny by the Commissioner as the Commissioner may require:

- all applications made for warrants complying with Article 12(1) and applications made for the renewal of such warrants.
- all warrants, and renewals and copies of schedule modifications (if any).
- where any application is refused, the grounds for refusal as given by the Attorney General.
- the dates on which interception is started and stopped.

4.18 Records shall also be kept of the arrangements by which the requirements of Article 19(2) (minimisation of copying and destruction of intercepted material) and Article 19(3) (destruction of intercepted material) are to be met. For further details see chapter on "Safeguards".

4.19 The term "intercepted material" is used throughout to embrace copies, extracts or summaries made from the intercepted material as well as the intercept material itself.

5 INTERCEPTION WARRANTS (ARTICLE 12(4))

5.1 This chapter applies to the interception of external communications by means of a warrant complying with Article 12(4) of the Law. External communications are those which are sent or received outside Jersey. They include those which are both sent and received outside Jersey, whether or not they pass through Jersey in course of their transit. They do not include communications both sent and received in Jersey, even if they pass outside Jersey en route. Responsibility for the issuing of such interception warrants rests with the Attorney General.

Application for an Article 12(4) Warrant

5.2 An application for a warrant is made to the Attorney General. Interception warrants, when issued, are addressed to the person who submitted the application. This person may then serve a copy upon any person who may be able to provide assistance in giving effect to that warrant. Each application, a copy of which must be retained by the applicant, should contain the following information:

- Background to the operation in question.
- Description of the communications to be intercepted, details of the communications service provider(s) and an assessment of the feasibility of the operation where this is relevant.

- Description of the conduct to be authorized, which must be restricted to the interception of external communications, or to conduct necessary in order to intercept those external communications, where appropriate.
- The certificate that will regulate examination of intercepted material.
- An explanation of why the interception is considered to be necessary for one or more of the Article 10(3) purposes.
- A consideration of why the conduct to be authorized by the warrant is proportionate to what is sought to be achieved by that conduct.
- A consideration of any unusual degree of collateral intrusion, and why that intrusion is justified in the circumstances. In particular, where the communications in question might affect religious, medical or journalistic confidentiality or legal privilege, this must be specified in the application.
- Where an application is urgent, supporting justification should be provided.
- An assurance that intercepted material will be read, looked at or listened to only so far as it is certified, and it meets the conditions of Articles 20(2) - (6) of the Law.
- An assurance that all material intercepted will be handled in accordance with the safeguards required by Articles 19 and 20 of the Law.

Authorization of an Article 12(4) warrant

5.3 Before issuing a warrant under Article 12(4), the Attorney General must believe that the warrant is necessary:

- in the interests of national security;
- for the purpose of preventing or detecting serious crime; or
- for the purpose of safeguarding the economic well-being of Jersey;

5.4 In exercising the Attorney General's power to issue an interception warrant for the purpose of safeguarding the economic well-being of Jersey (as provided for by Article 10(3)(c) of the Law), the Attorney General will consider whether the economic well-being of Jersey which is to be safeguarded is, on the facts of each case, directly related to national security. The Attorney General will not issue a warrant on Article 10(3)(c) grounds if this direct link between the economic well-being of Jersey and national security is not established. Any application for a warrant on Article 10(3)(c) grounds should therefore explain how, in the applicant's view, the economic well-being of Jersey which is to be safeguarded is directly related to national security on the facts of the case.

5.5 The Attorney General must also consider that the conduct authorized by the warrant is proportionate to what it seeks to achieve (Article 10(2)(b)). In considering necessity and proportionality, the Attorney General must take into account whether the information sought could reasonably be obtained by other means (Article 10(4)).

5.6 When the Attorney General issues a warrant of this kind, it must be accompanied by a certificate in which the Attorney General certifies that he or she considers examination of the intercepted material to be necessary for one or more of the Article 10(3) purposes. The Attorney General has a duty to ensure that arrangements are in force for securing that only that material which has been certified as necessary for examination for an Article 10(3) purpose, and which meets the conditions set out in Article 20(2) to (6) is, in fact, read, looked at or listened to. The Commissioner is under a duty to review the adequacy of those arrangements.

Format of an Article 12(4) Warrant

5.7 Each warrant is addressed to the person who submitted the application. This person may then serve a copy upon such providers of communications services as the person believes will be able to assist in implementing the interception. Communications service providers will not receive a copy of the certificate.

- The warrant should include the following:
  - A description of the communications to be intercepted
  - The warrant reference number
  - The persons who may subsequently modify the scheduled part of the warrant in an urgent case (if authorized in accordance with Article 14(5) of the Law).

Modification of an Article 12(4) warrant

5.8 Interception warrants may be modified by the Attorney General under the provisions of Article 14. The modification will expire at the same time as the warrant.

5.9 The certificate may be modified by the Attorney General. The modification expires on the expiry of the warrant.

Renewal of an Article 12(4) Warrant

5.10 The Attorney General may renew a warrant at any point before its expiry date. Applications for renewals are made to the Attorney General and contain an update of the matters outlined in paragraph 5.2 above. In particular, the applicant must give an assessment of the value of interception to the operation to date and explain why the applicant considers that interception continues to be necessary for one or more of purposes in Article 10(3).

5.11 Where the Attorney General is satisfied that the interception continues to meet the requirements of the Law the Attorney General may renew the warrant. Where the warrant is issued on serious crime grounds, the renewed warrant is valid for a further 3 months. Where it is issued on national security/ economic well-being grounds the renewed warrant is valid for 6 months. These dates run from the date of signature on the renewal instrument.

5.12 In those circumstances where the assistance of communications service providers has been sought, a copy of the warrant renewal instrument will be forwarded by the intercepting agency to all those on whom a copy of

the original warrant instrument has been served, providing they are still actively assisting. A warrant renewal instrument will include the reference number of the warrant and description of the communications to be intercepted.

Warrant Cancellation

5.13 The Attorney General shall cancel an interception warrant if, at any time before its expiry date, the Attorney General is satisfied that the warrant is no longer necessary on grounds falling within Article 10(3) of the Law.

5.14 The cancellation instrument will be addressed to the person to whom the warrant was issued (the intercepting agency). A copy of the cancellation instrument should be sent to those communications service providers, if any, who have given effect to the warrant during the preceding 12 months.

Records

5.15 The independent scrutiny régime allows the Commissioner to inspect the warrant application upon which the Attorney General based his or her decision, and the applicant may be required to justify the content. Each intercepting agency should keep, so to be made available for scrutiny by the Commissioner, the following:

- all applications made for warrants complying with Article 12(4), and applications made for the renewal of such warrants.
- all warrants and certificates, and copies of renewal and modification instruments (if any).
- where any application is refused, the grounds for refusal as given by the Attorney General.
- the dates on which interception is started and stopped.

Records shall also be kept of the arrangements in force for securing that only material which has been certified for examination for a purpose under Article 10(3) and which meets the conditions set out in Article 20(2) to (6) of the Law in accordance with Article 19 of the Law. Records shall be kept of the arrangements by which the requirements of Article 19(2) (minimisation of copying and distribution of intercepted material) and Article 19(3) (destruction of intercepted material) are to be met. For further details see chapter on "Safeguards".

6 SAFEGUARDS

6.1 All material (including related communications data) intercepted under the authority of a warrant complying with Article 12(1) or Article 12(4) of the Law must be handled in accordance with safeguards which the Attorney General has approved in conformity with the duty imposed upon the Attorney General by the Law. These safeguards are made available to the Commissioner, and they must meet the requirements of Article 19 of the Law which are set out below. In addition, the safeguards in Article 20 of the Law apply to warrants complying with Article 12(4). Any breach of these safeguards must be reported to the Commissioner.

6.2 Article 19 of the Law requires that disclosure, copying and retention of intercept material be limited to the minimum necessary for the authorized purposes. The authorized purposes defined in Article 19(4) of the Law include:

- if the material continues to be, or is likely to become, necessary for any of the purposes set out in Article 10(3) - namely, in the interests of national security, for the purpose of preventing or detecting serious crime, for the purpose of safeguarding the economic well-being of Jersey.
- if the material is necessary for facilitating the carrying out of the functions of the Attorney General under Chapter 1 of Part 2 of the Law.
- if the material is necessary for facilitating the carrying out of any functions of the Commissioner or the Tribunal.
- if the material is necessary to ensure that a person conducting a criminal prosecution has the information he or she needs to determine what is required of the person by his or her duty to secure the fairness of the prosecution.

6.3 Article 20 provides for additional safeguards in relation to material gathered under Article 12(4) warrants, requiring that the safeguards:

- ensure that intercepted material is read, looked at or listened to by any person only to the extent that the material is certified.
- regulate the use of selection factors that refer to individuals known to be for the time being in Jersey.

The Attorney General must ensure that the safeguards are in force before any interception under warrants complying with Article 12(4) can begin. The Commissioner is under a duty to review the adequacy of the safeguards.

Dissemination of Intercepted Material

6.4 The number of persons to whom any of the material is disclosed, and the extent of disclosure, must be limited to the minimum that is necessary for the authorized purposes set out in Article 19(4) of the Law. This obligation applies equally to disclosure to additional persons within an agency, and to disclosure outside the agency. It is enforced by prohibiting disclosure to persons who do not hold the required security clearance, and also by the need-to-know principle: intercepted material must not be disclosed to any person unless that person's duties, which must relate to one of the authorized purposes, are such that the person needs to know about the material to carry out those duties. In the same way only so much of the material may be disclosed as the recipient needs; for example if a summary of the material will suffice, no more than that should be disclosed.

6.5 The obligations apply not just to the original interceptor, but also to anyone to whom the material is subsequently disclosed. In some cases this will be achieved by requiring the latter to obtain the originator's permission before disclosing the material further. In others, explicit safeguards are applied to secondary recipients.

Copying

6.6 Intercepted material may only be copied to the extent necessary for the authorized purposes set out in Article 19(4) of the Law. Copies include not only direct copies of the whole of the material, but also extracts and summaries which identify themselves as the product of an interception, and any record referring to an interception which is a record of the identities of the persons to or by whom the intercepted material was sent. The restrictions are implemented by requiring special treatment of such copies, extracts and summaries that are made by recording their making, distribution and destruction.

Storage

6.7 Intercepted material, and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss or theft. It must be held so as to be inaccessible to persons without the required level of security clearance. This requirement to store intercept product securely applies to all those who are responsible for the handling of this material, including communications service providers. The details of what such a requirement will mean in practice for communications service providers will be set out in the discussions they will be having with the law enforcement agency before an Article 16 Notice is served (see paragraph 2.9).

Destruction

6.8 Intercepted material, and all copies, extracts and summaries which can be identified as the product of an interception, must be securely destroyed as soon as it is no longer needed for any of the authorized purposes. If such material is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid under Article 19(3) of the Law.

Personnel security

6.9 Each intercepting agency maintains a distribution list of persons who may have access to intercepted material or need to see any reporting in relation to it. All such persons must be appropriately vetted. Any person no longer needing access to perform his or her duties should be removed from any such list. Where it is necessary for an officer of one agency to disclose material to another, it is the former's responsibility to ensure that the recipient has the necessary clearance.

7 DISCLOSURE TO ENSURE FAIRNESS IN CRIMINAL PROCEEDINGS

7.1 Article 19(3) of the Law states the general rule that intercepted material must be destroyed as soon as its retention is no longer necessary for a purpose authorized under the Law. Article 19(4) specifies the authorized purposes for which retention is necessary.

7.2 This part of the Code applies to the handling of intercepted material in the context of criminal proceedings where the material has been retained for one of the purposes authorized in Article 19(4) of the Law. For those who would ordinarily have had responsibility to provide disclosure in criminal

proceedings, this includes those rare situations where destruction of intercepted material has not taken place in accordance with Article 19(3) and where that material is still in existence after the commencement of a criminal prosecution, retention having been considered necessary to ensure that a person conducting a criminal prosecution has the information he or she needs to discharge his or her duty of ensuring its fairness (Article 19(4)(d)).

Exclusion of Matters from Legal Proceedings

7.3 The general rule is that neither the possibility of interception nor intercepted material itself plays any part in legal proceedings. This rule is set out in Article 21 of the Law, which excludes evidence, questioning, assertion or disclosure in legal proceedings likely to reveal the existence (or the absence) of a warrant issued under this Law (or the Interception of Communications (Jersey) Law 1993). This rule means that the intercepted material cannot be used either by the prosecution or the defence. This preserves "equality of arms" which is a requirement under Article 6 of the European Convention on Human Rights.

7.4 Article 22 contains a number of tightly-drawn exceptions to this rule. This part of the Code deals only with the exceptions in paragraphs (7) to (10).

Disclosure to a Prosecutor

7.5 Article 22(7)(a) provides that intercepted material obtained by means of a warrant and which continues to be available, may, for a strictly limited purpose, be disclosed to a person conducting a criminal prosecution.

7.6 This may only be done for the purpose of enabling the prosecutor to determine what is required of the prosecutor by his or her duty to secure the fairness of the prosecution. The prosecutor may not use intercepted material to which he or she is given access under Article 22(7)(a) to mount a cross-examination, or to do anything other than ensure the fairness of the proceedings.

7.7 The exception does not mean that intercepted material should be retained against a remote possibility that it might be relevant to future proceedings. The normal expectation is, still, for the intercepted material to be destroyed in accordance with the general safeguards provided by Article 19. The exceptions only come into play if such material has, in fact, been retained for an authorized purpose. Because the authorized purpose given in Article 10(3)(b) ("*for the purpose of preventing or detecting serious crime*") does not extend to gathering evidence for the purpose of a prosecution, material intercepted for this purpose may not have survived to the prosecution stage, as it will have been destroyed in accordance with the Article 19(3) safeguards. There is, in these circumstances, no need to consider disclosure to a prosecutor if, in fact, no intercepted material remains in existence.

7.8 Be that as it may, Article 22(7)(a) recognises the duty on prosecutors, to review all available material to make sure that the prosecution is not proceeding unfairly. 'Available material' will only ever include intercepted material at this stage if the conscious decision has been made to retain it for an authorized purpose.

7.9 If intercepted material does continue to be available at the prosecution stage, once this information has come to the attention of the holder of this material the prosecutor should be informed that a warrant has been issued under Article 10 and that material of possible relevance to the case has been intercepted.

7.10 Having had access to the material, the prosecutor may conclude that the material affects the fairness of the proceedings. In these circumstances, the prosecutor will decide how the prosecution, if it proceeds, should be presented.

Disclosure to the Bailiff

7.11 Article 22(7)(b) recognises that there may be cases where the prosecutor, having seen intercepted material under paragraph (7)(a), will need to consult the judge presiding at the trial. Accordingly, it provides for the Bailiff to be given access to intercepted material, where there are exceptional circumstances making that disclosure essential in the interests of justice.

7.12 This access will be achieved by the prosecutor inviting the Bailiff to make an order for disclosure to the Bailiff alone, under this paragraph. This is an exceptional procedure; normally, the prosecutor's functions under paragraph (7)(a) will not fall to be reviewed by the Bailiff. To comply with Article 21(1), any consideration given to, or exercise of, this power must be carried out without notice to the defence. The purpose of this power is to ensure that the trial is conducted fairly.

7.13 The Bailiff may, having considered the intercepted material disclosed to the Bailiff, direct the prosecution to make an admission of fact. The admission will be abstracted from the interception; but, in accordance with the requirements of Article 21(1), it must not reveal the fact of interception. This is likely to be a very unusual step. The Law only allows it where the Bailiff considers it essential in the interests of justice.

7.14 Nothing in these provisions allows intercepted material, or the fact of interception, to be disclosed to the defence.

8 OVERSIGHT

8.1 The Law provides for a Commissioner whose remit is to provide independent oversight of the use of the powers contained within the warranted interception régime under Chapter 1 of Part 2 of the Law.

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 above powers to comply with any request made by the Commissioner to provide any information as the Commissioner requires for the purpose of enabling the Commissioner to discharge his or her functions.

9 COMPLAINTS

9.1 The Law establishes an independent Tribunal. This Tribunal will be made up of a judge of the Court of Appeal and 2 Jurats and is independent of

the States. 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. Details of the relevant complaints procedure can be obtained from:

The Judicial Greffier

Morier House

St Helier

Jersey

JE1 1DD

10 INTERCEPTION WITHOUT A WARRANT

10.1 Article 8(4) of the Law permits interception without a warrant in the following circumstances:

- where it is authorized by or under Article 8 or 9 of the Law (see below);
- where it is in exercise, in relation to any stored communication, of some other statutory power exercised for the purpose of obtaining information or of taking possession of any document or other property, for example, the obtaining of a production order under Schedule 1 to the Police Procedures and Criminal Evidence (Jersey) Law 2003 for stored data to be produced.

Interception in accordance with a warrant under Article 10 of the Law is dealt with under Chapters 2, 3, 4 and 5 of this Code.

10.2 For lawful interception which takes place without a warrant, pursuant to Articles 8 or 9 of the Law or pursuant to some other statutory power, there is no prohibition in the Law on the evidential use of any material that is obtained as a result. The matter may still, however, be regulated by the exclusionary rules of evidence to be found in the customary law, Article 76 of the Police Procedures and Criminal Evidence (Jersey) Law 2003, and/or pursuant to the Human Rights (Jersey) Law 2000.

Interception with the Consent of both Parties

10.3 Article 8(1) of the Law authorizes the interception of a communication if both the person sending the communication and the intended recipient(s) have consented to its interception, or where the person conducting the interception has reasonable grounds for believing that all parties have consented to the interception.

Interception with the Consent of one Party

10.4 Article 8(2) of the Law authorizes the interception of a communication if either the sender or intended recipient of the communication has consented to its interception, and directed surveillance by means of that interception has been authorized under Part 3 of the Law. Further details can be found in Chapter 4 of the Covert Surveillance Code of Practice and in Chapter 2 of the Covert Human Intelligence Sources Code of Practice.

Interception for the Purposes of a Communication Service Provider

10.5 Article 8(3) of the Law permits a communication service provider or a person acting upon a provider's behalf to carry out interception for purposes connected with the operation of that service or for purposes connected with the enforcement of any enactment relating to the use of the communication service.

Lawful Business Practice

10.6 Article 9(2) of the Law enables the Minister for Home Affairs to make an Order setting out those circumstances where it is lawful to intercept communications for the purpose of carrying on a business. This Order applies equally to public authorities.

SCHEDULE 2

(Article 2)

CODE OF PRACTICE ON INTERCEPTION OF COMMUNICATIONS – POSTAL

CONTENTS

1 GENERAL

1.1 This Code of Practice relates to the powers and duties conferred or imposed under Chapter 1 of Part 3 of the Regulation of Investigatory Powers (Jersey) Law 2005 (the "Law"). It provides guidance on the procedures that must be followed before interception of postal communications can take place under those provisions. It is primarily intended for use by those public authorities listed in Article 11(1) of the Law. It will also prove useful to postal operators and other interested bodies to acquaint themselves with the procedures to be followed by those public authorities.

1.2 The Law provides that all Codes of Practice relating to the Law are admissible as evidence in criminal and civil proceedings. If any provision of this Code appears relevant before any court or tribunal considering 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.

2 GENERAL RULES ON INTERCEPTION WITH A WARRANT

2.1 There are a limited number of persons by whom, or on behalf of whom, applications for interception warrants may be made. These persons are:

- The Chief Officer of the States Police;
- The Agent of the Impôts;
- The Chief Immigration Officer;
- The Intelligence Services;
- A person who, for the purposes of any international mutual assistance agreement, is the competent authority of a country or territory outside Jersey.

2.2 All interception warrants are issued by the Attorney General. Before issuing an interception warrant, the Attorney General must believe that what the action seeks to achieve is necessary for one of the following Article 10 purposes:

- in the interests of national security;
- for the purpose of preventing or detecting serious crime; or
- for the purpose of safeguarding the economic well-being of Jersey;

and that the conduct authorized by the warrant is proportionate to what is sought to be achieved by that conduct.

Necessity and Proportionality

2.3 Obtaining a warrant under the Law will only ensure that the interception authorized is a justifiable interference with an individual's rights under Article 8 of the European Convention of Human Rights (the right to privacy) if it is necessary and proportionate for the interception to take place. The Law recognises this by first requiring that the Attorney General believes that the authorization is necessary on one or more of the statutory grounds set out in Article 10 of the Law. This requires the Attorney General to believe that it is necessary to undertake the interception which is to be authorized for a particular purpose falling within the relevant statutory ground.

2.4 Then, if the interception is necessary, the Attorney General must also believe that it is proportionate to what is sought to be achieved by carrying it out. This involves balancing the intrusiveness of the interference, against the need for it in operational terms. Interception of communications will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other means. Further, all interception should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

Implementation of Warrants

2.5 After a warrant has been issued it will be forwarded to the person to whom it is addressed, which in practice will be the person or agency that submitted the application. The Law (Article 15) then permits the intercepting agency to carry out the interception, or to require the

assistance of other persons in giving effect to the warrant. Warrants cannot be served on those outside Jersey.

Provision of Reasonable Assistance

2.6 Any public postal operator in Jersey may be required to provide assistance in giving effect to an interception. The Law places a requirement on postal operators to take all such steps for giving effect to the warrant as are notified to them (Article 15(4) of the Law). But the steps that may be required are limited to those which it is reasonably practicable to take (Article 15(5)). If there is disagreement about what is reasonably practicable, it will be for the Attorney General to decide whether to press forward with civil proceedings or whether to institute criminal proceedings.

2.7 Where the intercepting agency requires the assistance of a postal operator in order to implement a warrant, the agency should provide the following to the postal operator:

- A copy of the warrant instrument signed and dated by the Attorney General;
- The relevant schedule for that service provider setting out the addresses or other factors identifying the communications to be intercepted;
- A covering document from the intercepting agency requiring the assistance of the postal operator and specifying any other details regarding the means of interception and delivery as may be necessary. Contact details with respect to the intercepting agency will either be provided in this covering document or will be available in the handbook provided to all postal operators who maintain an intercept capability.

Provision of Intercept Capability

2.8 Whilst all persons who provide a postal service are obliged to provide assistance in giving effect to an interception, persons who provide a public postal service, or plan to do so, may also be required to provide a reasonable intercept capability. The obligations that the Minister for Home Affairs considers reasonable to impose on such persons to ensure they have such a capability will be set out in an Order made by the Minister for Home Affairs following wider consultation. A notice may be served upon a postal operator setting out the steps they must take to ensure they can meet these obligations. A notice will not be served without consultation over the content of the notice between the law enforcement agencies and the postal service provider having previously taken place. When served with such a notice, a postal operator, if the operator feels it unreasonable, will be able to refer that notice to the Technical Advisory Board on the reasonableness of the technical requirements and capabilities that are being sought. Details of how to submit a notice to the Board will be provided either before or at the time the notice is served.

2.9 Any postal operator obliged to maintain a reasonable intercept capability will be provided with instructions or a handbook which will contain the

basic information they require to respond to requests for reasonable assistance for the interception of communications.

Duration of Interception Warrants

2.10 All interception warrants are valid for an initial period of 3 months. Upon renewal, warrants issued on serious crime grounds are valid for a further period of 3 months. Warrants renewed on national security/economic well-being grounds are valid for a further period of 6 months.

2.11 Where a change in circumstance prior to the set expiry date leads the intercepting agency to consider it no longer necessary or practicable for the warrant to be in force, it should be cancelled with immediate effect.

Stored Communications

2.12 Article 2(7) of the Law defines a communication in the course of its transmission as also encompassing any time when the communication is being stored in the communication system.

2.13 Stored communications may also be accessed by means other than a warrant. If a communication has been stored within a transit system it may be obtained with lawful authority by means of an existing statutory power such as a production order (*e.g.* under the Police Procedures and Criminal Evidence (Jersey) Law, 2003) or a search warrant.

3 SPECIAL RULES ON INTERCEPTION WITH A WARRANT

Collateral Intrusion

3.1 Consideration should be given to any infringement of the privacy of individuals who are not the subject of the intended interception, especially where communications relating to religious, medical, journalistic or legally privileged material may be involved. An application for an interception warrant should draw attention to any circumstances which give rise to an unusual degree of collateral infringement of privacy, and this will be taken into account by the Attorney General when considering a warrant application. Should an interception operation reach the point where individuals other than the subject of the authorization are identified as directly relevant to the operation, consideration should be given to applying for separate warrants covering those individuals.

Confidential Information

3.2 Particular consideration should also be given in cases where the subject of the interception might reasonably assume a high degree of privacy, or where confidential information is involved. Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material (see paragraphs 3.9-3.11). For example, extra consideration should be given where interception might involve communications between a minister of religion and an individual relating to the latter's spiritual welfare, or where matters of medical or journalistic confidentiality or legal privilege may be involved.

Communications Subject to Legal Privilege

3.3 Article 5 of the Police Procedures and Criminal Evidence (Jersey) Law 2003 describes those matters that are usually regarded as subject to legal privilege. Legal privilege does not apply to communications made with the intention of furthering a criminal purpose (whether the lawyer is acting unwittingly or culpably). Legally privileged communications will lose their protection if there are grounds to believe, for example, that the lawyer is intending to hold or use the information for a criminal purpose. But privilege is not lost if a lawyer is properly advising a person who is suspected of having committed a criminal offence. The concept of legal privilege applies to the provision of professional legal advice by any individual, agency or organisation qualified to do so.

3.4 The Law does not provide any special protection for legally privileged communications. Nevertheless, intercepting such communications is particularly sensitive and is therefore subject to additional safeguards under this Code. The guidance set out below may in part depend on whether matters subject to legal privilege have been obtained intentionally or incidentally to some other material which has been sought.

3.5 In general, any application for a warrant which is likely to result in the interception of legally privileged communications should include, in addition to the reasons why it is considered necessary for the interception to take place, an assessment of how likely it is that communications which are subject to legal privilege will be intercepted. In addition, it should state whether the purpose (or one of the purposes) of the interception is to obtain privileged communications. This assessment will be taken into account by the Attorney General in deciding whether an interception is necessary under Article 10 of the Law and whether it is proportionate. In such circumstances, the Attorney General will be able to impose additional conditions such as regular reporting arrangements so as to be able to exercise his or her discretion on whether a warrant should continue to be authorized. In those cases where communications which include legally privileged communications have been intercepted, the matter should be reported to the Commissioner during his or her inspections and the material be made available to the Commissioner if requested.

3.6 Where an Advocate or Solicitor or other professional legal adviser is the subject of an interception, it is possible that a substantial proportion of the communications which will be intercepted will be between the lawyer and his or her client(s) and will be subject to legal privilege. Any case where a lawyer is the subject of an investigation should be notified to the Commissioner during the Commissioner's inspections and any material which has been retained should be made available to the Commissioner if requested.

3.7 In addition to the safeguards governing the handling and retention of intercept material as provided for in Article 19 of the Law, persons who examine intercepted communications should be alert to any intercept material which may be subject to legal privilege. Where there is doubt as to whether the communications are subject to legal privilege, advice should be sought from the Law Officers Department. Similarly, advice

should also be sought where there is doubt over whether communications are not subject to legal privilege due to the "in furtherance of a criminal purpose" exception.

Communications involving Confidential Personal Information and Confidential Journalistic Material

3.8 Similar consideration to that given to legally privileged communications must also be given to the interception of communications that involve confidential personal information and confidential journalistic material. Confidential personal information is information held in confidence concerning an individual (whether living or dead) who can be identified from it, and the material in question relates to his physical or mental health or to spiritual counselling. Such information can include both oral and written communications. Such information as described above is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. For example, confidential personal information might include consultations between a health professional and a patient, or information from a patient's medical records.

3.9 Spiritual counselling is defined as conversations between an individual and a Minister of Religion acting in his or her official capacity, and where the individual being counselled is seeking or the Minister is imparting forgiveness, absolution or the resolution of conscience with the authority of the Divine Being(s) of their particular faith.

3.10 Confidential journalistic material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.

4 INTERCEPTION WARRANTS (ARTICLE 12(1))

4.1 This Chapter applies to the interception of communications by means of a warrant complying with Article 12(1) of the Law. This type of warrant may be issued in respect of the interception of communications carried on any postal service as defined in Article 1(1) of the Law. Responsibility for the issuing of interception warrants rests with the Attorney General.

Application for a Article 12(1) Warrant

4.2 An application for a warrant is made to the Attorney General. Interception warrants, when issued, are addressed to the person who submitted the application. This person may then serve a copy upon any person who may be able to provide assistance in giving effect to that warrant. Each application, a copy of which must be retained by the applicant, should contain the following information:

- Background to the operation in question.
- Person or premises to which the application relates (and how the person or premises feature in the operation).

- Description of the communications to be intercepted, details of the postal operator(s) and an assessment of the feasibility of the interception operation where this is relevant.
- Description of the conduct to be authorized as considered necessary in order to carry out the interception, where appropriate.
- An explanation of why the interception is considered to be necessary under the provisions of Article 10.
- A consideration of why the conduct to be authorized by the warrant is proportionate to what is sought to be achieved by that conduct.
- A consideration of any unusual degree of collateral intrusion and why that intrusion is justified in the circumstances. In particular, where the communications in question might affect religious, medical or journalistic confidentiality or legal privilege, this must be specified in the application.
- Where an application is urgent, supporting justification should be provided.
- An assurance that all material intercepted will be handled in accordance with the safeguards required by Article 19 of the Law.

Authorization of an Article 12(1) Warrant

4.3 Before issuing a warrant under Article 12(1), The Attorney General must believe the warrant is necessary:

- in the interests of national security;
- for the purpose of preventing or detecting serious crime; or
- for the purpose of safeguarding the economic well-being of Jersey.

4.4 In exercising his or her power to issue an interception warrant for the purpose of safeguarding the economic well-being of Jersey (as provided for by Article 10 of the Law), the Attorney General will consider whether the economic well-being of Jersey which is to be safeguarded is, on the facts of each case, directly related to national security. The Attorney General will not issue a warrant on Article 10 grounds if this direct link between the economic well-being of Jersey and national security is not established. Any application for a warrant on Article 5(3)(c) grounds should therefore explain how, in the applicant's view, the economic well-being of Jersey which is to be safeguarded is directly related to national security on the facts of the case.

4.5 The Attorney General must also consider that the conduct authorized by the warrant is proportionate to what it seeks to achieve (Article 10). In considering necessity and proportionality, the Attorney General must take into account whether the information sought could reasonably be obtained by other means (Article 10).

Format of an Article 12 Warrant

4.6 Each warrant comprises 2 sections, a warrant instrument signed by the Attorney General listing the subject of the interception or the set of premises, a copy of which each postal operator will receive, and a schedule or set of schedules listing the communications to be intercepted.

Only the schedule relevant to the communications that can be intercepted by the specified postal operator will be provided to that service provider.

4.7 The warrant instrument should include:

- The name or description of the interception subject or of a set of premises in relation to which the interception is to take place;
- A warrant reference number.

4.8 The scheduled part of the warrant will comprise one or more schedules. Each schedule should contain:

- The name of the postal operator, or the other person who is to take action;
- A warrant reference number;
- A means of identifying the communications to be intercepted.

Modification of Article 7(1) warrant

4.9 Interception warrants may be modified under the provisions of Article 14 of the Law. The unscheduled part of a warrant may only be modified by the Attorney General. The modification will expire on the expiry date of the warrant.

4.10 Scheduled parts of a warrant may be modified by the Attorney General in which case the modification expires on the expiry date of the warrant. A modification to the scheduled part of the warrant may include the addition of a new schedule relating to a communication service provider or when a copy of the warrant has not been previously served. In an urgent case, where the warrant specifically authorizes it, scheduled parts of a warrant may be modified by the person to whom the warrant is addressed (the person who submitted the application) or a subordinate (where the subordinate is identified in the warrant). Modifications of this kind are valid for 5 working days following the day of issue unless the modification instrument is endorsed by the Attorney General. Where the modification is endorsed in this way, the modification expires upon the expiry date of the warrant.

4.11 There is a duty to modify a warrant by deleting a communications identifier if it is no longer relevant. When a modification is sought to delete a number or other communication identified, the relevant communication service provider must be advised and the interception suspended before the modification is made.

Renewal of Article 12(1) Warrant

4.12 The Attorney General may renew a warrant at any point before its expiry date. Applications for renewals must be made to the Attorney General and should contain an update of the matters outlined in paragraph 4.2. In particular, the applicant should give an assessment of the value of interception to the operation to date and explain why he considers that interception continues to be necessary for one or more of the purposes in Article 10(3).

4.13 Where the Attorney General is satisfied that the interception continues to meet the requirements of the Law the Attorney General may renew the

warrant. Where the warrant is issued on serious crime grounds, the renewed warrant is valid for a further 3 months. Where it is issued on national security/economic well-being grounds, the renewed warrant is valid for 6 months. These dates run from the date of signature on the renewal instrument.

4.14 A copy of the warrant renewal instrument will be forwarded by the intercepting agency to all relevant communications service providers on whom a copy of the original warrant instrument and a schedule have been served, providing they are still actively assisting. A warrant renewal instrument will include the reference number of the warrant and description of the person or premises described in the warrant.

Warrant Cancellation

4.15 The Attorney General is under a duty to cancel an interception warrant if, at any time before its expiry date, he or she is satisfied that the warrant is no longer necessary on grounds falling within Article 10(3) of the Law. Intercepting agencies will therefore need to keep their warrants under continuous review.

4.16 The cancellation instrument should be addressed to the person to whom the warrant was issued (the intercepting agency) and should include the reference number of the warrant and the description of the person or premises specified in the warrant. A copy of the cancellation instrument should be sent to those communications service providers who have held a copy of the warrant instrument and accompanying schedule during the preceding 12 months.

Records

4.17 The independent scrutiny régime allows the Commissioner appointed under the Law to inspect the warrant application on which the Attorney General based his or her decision and the applicant may be required to justify the content. Each intercepting agency should keep the following to be made available for scrutiny by the Commissioner as he may require:

- all applications made for warrants complying with Article 12(1) and applications made for the renewal of such warrants.
- all warrants, and renewals and copies of schedule modifications (if any).
- where any application is refused, the grounds for refusal as given by the Attorney General.
- the dates on which interception is started and stopped.

4.18 Records shall also be kept of the arrangements by which the requirements of Article 19(2) (minimisation of copying and destruction of intercepted material) and Article 19(3) (destruction of intercepted material) are to be met. For further details see chapter on “Safeguards”.

4.19 The term “intercepted material” is used throughout to embrace copies, extracts or summaries made from the intercepted material as well as the intercept material itself.

5 SAFEGUARDS

5.1 All material (including related communications data) intercepted under the authority of a warrant complying with Article 12(1) of the Law must be handled in accordance with safeguards which the Attorney General has approved in conformity with the duty imposed upon the Attorney General by the Law. These safeguards are made available to the Commissioner, and they must meet the requirements of Article 19 of the Law which are set out below. Any breach of these safeguards must be reported to the Commissioner.

5.2 Article 19 of the Law requires that disclosure, copying and retention of intercept material be limited to the minimum necessary for the authorized purposes. The authorized purposes defined in Article 19(4) of the Law include:

- if the material continues to be, or is likely to become, necessary for any of the purposes set out in Article 10(3) - namely, in the interests of national security, for the purpose of preventing or detecting serious crime, for the purpose of safeguarding the economic well-being of Jersey.
- if the material is necessary for facilitating the carrying out of the functions of the Attorney General under Chapter I of Part 2 of the Law.
- if the material is necessary for facilitating the carrying out of any functions of the Commissioner or the Tribunal.
- if the material is necessary to ensure that a person conducting a criminal prosecution has the information he or she needs to determine what is required of the person by his or her duty to secure the fairness of the prosecution.

Dissemination of Intercepted Material

5.3 The number of persons to whom any of the material is disclosed, and the extent of disclosure, must be limited to the minimum that is necessary for the authorized purposes set out in Article 19(4) of the Law. This obligation applies equally to disclosure to additional persons within an agency, and to disclosure outside the agency. It is enforced by prohibiting disclosure to persons who do not hold the required security clearance, and also by the need-to-know principle: intercepted material must not be disclosed to any person unless that person's duties, which must relate to one of the authorized purposes, are such that he or she needs to know about the material to carry out those duties. In the same way only so much of the material may be disclosed as the recipient needs; for example if a summary of the material will suffice, no more than that should be disclosed.

5.4 The obligations apply not just to the original interceptor, but also to anyone to whom the material is subsequently disclosed. In some cases this will be achieved by requiring the latter to obtain the originator's permission before disclosing the material further. In others, explicit safeguards are applied to secondary recipients.

Copying

5.5 Intercepted material may only be copied to the extent necessary for the authorized purposes set out in Article 19(4) of the Law. Copies include not only direct copies of the whole of the material, but also extracts and summaries which identify themselves as the product of an interception, and any record referring to an interception which is a record of the identities of the persons to or by whom the intercepted material was sent. The restrictions are implemented by requiring special treatment of such copies, extracts and summaries that are made by recording their making, distribution and destruction.

Storage

5.6 Intercepted material, and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss or theft. It must be held so as to be inaccessible to persons without the required level of security clearance. This requirement to store intercept product securely applies to all those who are responsible for the handling of this material, including communications service providers. The details of what such a requirement will mean in practice for communications service providers will be set out in the discussions they will be having with the law enforcement agency before an Article 16 Notice is served (see paragraph 2.9).

Destruction

5.7 Intercepted material, and all copies, extracts and summaries which can be identified as the product of an interception, must be securely destroyed as soon as it is no longer needed for any of the authorized purposes. If such material is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid under Article 19(3) of the Law.

Personnel security

5.8 Each intercepting agency maintains a distribution list of persons who may have access to intercepted material or need to see any reporting in relation to it. All such persons must be appropriately vetted. Any person no longer needing access to perform his or her duties should be removed from any such list. Where it is necessary for an officer of one agency to disclose material to another, it is the former's responsibility to ensure that the recipient has the necessary clearance.

6 DISCLOSURE TO ENSURE FAIRNESS IN CRIMINAL PROCEEDINGS

6.1 Article 19(3) of the Law states the general rule that intercepted material must be destroyed as soon as its retention is no longer necessary for a purpose authorized under the Law. Article 19(4) specifies the authorized purposes for which retention is necessary.

6.2 This part of the Code applies to the handling of intercepted material in the context of criminal proceedings where the material has been retained for one of the purposes authorized in Article 19(4) of the Law. For those who would ordinarily have had responsibility to provide disclosure in criminal proceedings, this includes those rare situations where destruction of

intercepted material has not taken place in accordance with Article 19(3) and where that material is still in existence after the commencement of a criminal prosecution, retention having been considered necessary to ensure that a person conducting a criminal prosecution has the information he or she needs to discharge his duty of ensuring its fairness (Article 19(4)(d)).

Exclusion of Matters from Legal Proceedings

6.3 The general rule is that neither the possibility of interception nor intercepted material itself plays any part in legal proceedings. This rule is set out in Article 21 of the Law, which excludes evidence, questioning, assertion or disclosure in legal proceedings likely to reveal the existence (or the absence) of a warrant issued under this Law (or the Interception of Communications (Jersey) Law 1993). This rule means that the intercepted material cannot be used either by the prosecution or the defence. This preserves "equality of arms" which is a requirement under Article 6 of the European Convention on Human Rights.

6.4 Article 22 contains a number of tightly-drawn exceptions to this rule. This part of the Code deals only with the exceptions in paragraphs (7) to (10).

Disclosure to a Prosecutor

6.5 Article 22(7)(a) provides that intercepted material obtained by means of a warrant and which continues to be available, may, for a strictly limited purpose, be disclosed to a person conducting a criminal prosecution.

6.6 This may only be done for the purpose of enabling the prosecutor to determine what is required of the prosecutor by his or her duty to secure the fairness of the prosecution. The prosecutor may not use intercepted material to which he or she is given access under Article 22(7)(a) to mount a cross-examination, or to do anything other than ensure the fairness of the proceedings.

6.7 The exception does not mean that intercepted material should be retained against a remote possibility that it might be relevant to future proceedings. The normal expectation is, still, for the intercepted material to be destroyed in accordance with the general safeguards provided by Article 19. The exceptions only come into play if such material has, in fact, been retained for an authorized purpose. Because the authorized purpose given in Article 10(3)(b) ("*for the purpose of preventing or detecting serious crime*") does not extend to gathering evidence for the purpose of a prosecution, material intercepted for this purpose may not have survived to the prosecution stage, as it will have been destroyed in accordance with the Article 19(3) safeguards. There is, in these circumstances, no need to consider disclosure to a prosecutor if, in fact, no intercepted material remains in existence.

6.8 Be that as it may, Article 22(7)(a) recognises the duty on prosecutors, to review all available material to make sure that the prosecution is not proceeding unfairly. 'Available material' will only ever include intercepted material at this stage if the conscious decision has been made to retain it for an authorized purpose.

6.9 If intercepted material does continue to be available at the prosecution stage, once this information has come to the attention of the holder of this material the prosecutor should be informed that a warrant has been issued under Article 10 and that material of possible relevance to the case has been intercepted.

6.10 Having had access to the material, the prosecutor may conclude that the material affects the fairness of the proceedings. In these circumstances, the prosecutor will decide how the prosecution, if it proceeds, should be presented.

Disclosure to the Bailiff

6.11 Article 22(7)(b) recognises that there may be cases where the prosecutor, having seen intercepted material under paragraph (7)(a), will need to consult the judge presiding at the trial. Accordingly, it provides for the Bailiff to be given access to intercepted material, where there are exceptional circumstances making that disclosure essential in the interests of justice.

6.12 This access will be achieved by the prosecutor inviting the Bailiff to make an order for disclosure to the Bailiff alone, under this paragraph. This is an exceptional procedure; normally, the prosecutor's functions under paragraph (7)(a) will not fall to be reviewed by the Bailiff. To comply with Article 21(1), any consideration given to, or exercise of, this power must be carried out without notice to the defence. The purpose of this power is to ensure that the trial is conducted fairly.

6.13 The Bailiff may, having considered the intercepted material disclosed to the Bailiff, direct the prosecution to make an admission of fact. The admission will be abstracted from the interception; but, in accordance with the requirements of Article 21(1), it must not reveal the fact of interception. This is likely to be a very unusual step. The Law only allows it where the Bailiff considers it essential in the interests of justice.

6.14 Nothing in these provisions allows intercepted material, or the fact of interception, to be disclosed to the defence.

7 OVERSIGHT

7.1 The Law provides for a Commissioner whose remit is to provide independent oversight of the use of the powers contained within the warranted interception régime under Chapter I of Part 2 of the Law.

7.2 This Code does not cover the exercise of the Commissioner's functions. However, it will be the duty of any person who uses the above powers to comply with any request made by the Commissioner to provide any information as he or she requires for the purpose of enabling the prosecutor to discharge his or her functions.

8 COMPLAINTS

8.1 The Law establishes an independent Tribunal. This Tribunal will be made up of a judge of the Court of Appeal and 2 Jurats and is independent of

the States. The Tribunal has full powers to investigate and decide any case within its jurisdiction.

8.2 This code does not cover the exercise of the Tribunal's functions. Details of the relevant complaints procedure can be obtained from:

The Judicial Greffier

Morier House

St Helier

Jersey

JE1 1DD

9 INTERCEPTION WITHOUT A WARRANT

9.1 Article 7 of the Law permits interception without a warrant in the following circumstances:

- where it is authorized by or under Articles 8 or 9 of the Law (see below);
- where it is in exercise, in relation to any stored communication, of some other statutory power exercised for the purpose of obtaining information or of taking possession of any document or other property, for example, the obtaining of a production order under Schedule 2 to the Police Procedures and Criminal Evidence (Jersey) Law 2003 for stored data to be produced.

Interception in accordance with a warrant under Article 10 of the Law is dealt with under Chapters 2, 3 and 4 of this Code.

9.2 For lawful interception which takes place without a warrant, pursuant to Article 7 of the Law or pursuant to some other statutory power, there is no prohibition in the Law on the evidential use of any material that is obtained as a result. The matter may still, however, be regulated by the exclusionary rules of evidence to be found in the common law, in section 76 of the Police Procedures and Criminal Evidence (Jersey) Law 2003, and/or pursuant to the Human Rights (Jersey) Law 2000.

Interception with the consent of both parties

9.3 Article 8 of the Law authorizes the interception of a communication if both the person sending the communication and the intended recipient(s) have consented to its interception, or where the person conducting the interception has reasonable grounds for believing that all parties have consented to the interception.

Interception with the consent of one party

9.4 Article 8 of the Law authorizes the interception of a communication if either the sender or intended recipient of the communication has consented to its interception, and directed surveillance by means of that interception has been authorized under Part 2 of the Law. [Further details can be found in Chapter 4 of the Covert Surveillance Code of Practice and in Chapter 2 of the Covert Human Intelligence Sources Code of Practice].

Interception for the purposes of a postal operator

9.5 Article 8 of the Law permits a postal operator or a person acting upon their behalf to carry out interception for purposes connected with the operation of that service or for purposes connected with the enforcement of any enactment relating to the use of the postal service.

SCHEDULE 3

(Article 3)

CODE OF PRACTICE ON ACCESSING COMMUNICATIONS DATA

CONTENTS

1 INTRODUCTION

1.1 This Code of practice relates to the powers and duties conferred or imposed under Chapter 2 of Part 2 of the Regulation of Investigatory Powers (Jersey) Law 2005 (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 2 of Part 2 of the Law (see paragraph 3.1).

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

2 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 emails 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 authorized 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 2 of Part 2 of the Law (see paragraph 3.2). 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 the conduct involved in obtaining the communications data to be ***proportionate*** (see paragraph 4.4 below) to what it is sought to achieve.

3 DESIGNATED PERSONS WITHIN RELEVANT PUBLIC AUTHORITIES PERMITTED TO ACCESS COMMUNICATIONS DATA UNDER THE LAW

3.1 Designated persons within the following "*relevant public authorities*"[1] are permitted under the Law to grant authorizations or serve notices, the 2 routes by which the Law allows communications data to be accessed (see further paragraph 5.1):

- The States of Jersey Police Force;
- Immigration and Nationality Department;
- Customs and Excise;
- Income Tax Department;
- Any of the Parishes;
- Any of the Intelligence Services;

3.2 The Designated persons in respect of these bodies within each public authority for granting authorizations or giving notices will be as follows:

[1] The Law permits the States to add further public authorities to this list by means of Regulations.

- The States of Jersey Police : Chief Officer
- Immigration and Nationality Department : Chief Inspector
- Customs and Excise : Agent of the Impôts
- All others : the Attorney General

Relevant public authorities authorized to access communications data from the list in Chapter 2 of Part 2 of the Law may be removed, if deemed appropriate, by Regulations.

4 PURPOSES FOR WHICH COMMUNICATIONS DATA MAY BE SOUGHT

4.1 Under Article 26(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[2]:

- 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 Jersey (see paragraph 4.2 below);
- 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 the States;
- 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.

4.2 In exercising his or her power to grant an authorization or give a notice in the interests of the economic well-being of Jersey (as provided for by Article 26(2)(c)) of the Law, a designated person will consider whether the economic well-being of Jersey 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 authorization or give a notice on Article 26(2)(c) grounds if this link is not established. Any application for an authorization or a notice on Article 26(2)(c) grounds should therefore explain how, in the applicant's view, the economic well-being of Jersey which it is in the interests of is 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 a legitimate aim as listed in paragraph 4.1; fulfil a pressing social need and be proportionate to that aim.

4.4 Under Article 26(5) of the Law, a designated person must also consider the conduct involved in obtaining the communications data to be

[2] The Law permits the States to add further purposes to this list by means of Regulations.

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 a particular case which interferes with a Convention right[3] is aimed at pursuing a legitimate aim (as listed in paragraph 4.1 above) 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 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 an interference may still not be justified because the impact on the individual or group is too severe.

5 AUTHORIZATIONS AND NOTICES

5.1 The Law provides 2 different ways of authorizing access to communications data; through an authorization under Article 26(3) and by a notice under Article 26(4). An authorization 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. A designated person decides whether or not an authorization should be granted or a notice given.

5.2 In order to illustrate, an Article 26(3) authorization may be appropriate where:

- the postal or telecommunications operator is not capable of collecting or retrieving the communications data[4];
- 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.

5.3 Except where the Attorney General is the designated person, applications for communications data may 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 authorizations) for communications data should be channelled through single points of contact within each public authority (unless the exemption in paragraph 5.13 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 authorization or a notice is appropriate.

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

[3] European Convention on Human Rights (ECHR).
[4] Where possible, this assessment will be based upon information provided by the relevant postal or telecommunications operator.

- 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;
- advise applicants and designated persons on whether communications data falls under Article 24(a), (b) or (c) of the Law;
- provide safeguards for authentication;
- assess any cost and resource implications to both the public authority and the postal or telecommunications operator.

(b) Applications to obtain communications data under the Law

5.6 The application form is subject to inspection by the Commissioner and both the applicant and the 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 Chapter 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 (there will also be a need to identify whether it is communications data under Article 24(a), (b) or (c) 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, a consideration of 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 routine, the reasoning for this to 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 authorization or notice.

(c) Considerations for designated person

5.8 A designated person must take account of the following points, so that he or she is in a position to justify decisions made:

- whether the case justifies the accessing of communications data for one or more of the purposes listed in paragraph 4.1, and why obtaining the data is *necessary* for that purpose;
- whether obtaining access to the data by the conduct authorized by the authorization, 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 or she is authorizing or requiring in each case. In making a judgement as to proportionality, a designated person needs to have in mind whether he or she is granting an authorization 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 authorization

5.9 An authorization itself can only authorize conduct to which Chapter 2 of Part 2 of the Law applies. A designated person will make a decision whether to grant an authorization based upon the application which is made. The application form and the authorization itself is not served upon the holder of communications data. The authorization should be in a standard format (written or electronic) which must be retained by the public authority (see Chapter 7 of this Code) and must contain the following information:

- a description of the conduct to which Chapter 2 of Part 2 of the Law applies that is authorized;
- 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) or office of the designated person.

5.10 The authorization should also contain:

- a unique reference number.

(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) which must be retained by the public authority (see Chapter 7 of this Code) and must contain the following information:

- a description of the required communications data;
- for which of the purposes in paragraph 4.1 above the data is required;

- the name (or designation) and office of the designated person; and
- 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;
- a statement stating that data is sought under the provisions of Chapter 2 of Part 2 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 Article 26(2)(g) of the Law[5].

5.14 The fact of an oral application and approval must be reached by the applicant and designated person at the time or as soon as possible afterwards. In these circumstances, an authorization under Article 26(3) of the Law must be completed (in written or electronic format) as soon as practicable thereafter. In the case of a notice under Article 26(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 those urgent situations, an Article 26(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 Article 26(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.

6 VALIDITY OF AUTHORIZATIONS AND NOTICES

(a) Duration

6.1 Authorizations and notices will only be valid for one month. This period will begin when the authorization 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

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

'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 an Article 26(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 authorization or notice may be renewed at any time during the month it is valid, by following the same procedure as in obtaining a fresh authorization or notice.

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

(c) Cancellation

6.4 A designated person shall cancel a notice given under Article 26(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 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 is to be prescribed by the Minister for Home Affairs by Order.

6.6 As a matter of good practice, authorizations should also be cancelled in accordance with the procedure above.

6.7 In the case of an Article 26(4) notice, the relevant postal or telecommunications operator will be informed of the cancellation.

7 RETENTION OF RECORDS BY PUBLIC AUTHORITIES

7.1 Applications, authorizations 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 authorization or notice is started and cancelled.

(a) Errors

7.2 Where any errors have occurred in the granting of authorizations or the giving of notices, a record should be kept, and a report and explanation sent to the Commissioner as soon as is appropriate.

7.3 Applications must also be retained to allow for the complaints Tribunal, under Part 5 of the Law, to carry out its functions.

7.4 This Code does not affect any other legal obligations placed on public authorities to retain data under any other enactment.

(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 (Jersey) Law 2005 and its data protection principles should be adhered to[6].

8 OVERSIGHT

8.1 The Law provides for the Investigatory Powers Commissioner whose remit is to provide independent oversight of the use of the powers contained within Part 1.

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 2 of Part 2 to comply with any request made by the Commissioner to provide any information the Commissioner requires for the purposes of enabling him or her to discharge his functions.

9 COMPLAINTS

9.1 The Law establishes an independent Investigatory Powers Tribunal, which is made up of a Court of Appeal Judge and 2 Jurats and is independent of the States. 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 public offices of those public authorities permitted to access communications data under the provisions of Chapter 2 of Part 2 of the Law. Where this is not possible, copies should be made available by post or email.

[6] Further information and guidance is available from the Data Protection Office at www.dataprotection.gov.je

ANNEX A TO DRAFT CODE OF PRACTICE

Unique reference number: [*to be completed by the public authority*]

[*an indication of any urgency*]

NOTICE UNDER ARTICLE 26(4) OF THE REGULATION OF INVESTIGATORY POWERS (JERSEY) LAW 2005 REQUIRING COMMUNICATIONS DATA TO BE OBTAINED AND DISCLOSED

To: [NAME OF POSTAL OR TELECOMMUNICATIONS OPERATOR and address].

In accordance with Article 26(4) of the Regulation of Investigatory Powers (Jersey) Law 200-, 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 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 details of the communications data required {distinguish here between data (a) to be obtained if not already in the possession of the operator (omitting 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*]. This must be no more than one month from the date of this notice, or earlier if cancelled under Article 23(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:

[***List the purpose(s) that the communications data is required for (from Article 22(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 (a name or designation must be specified), office, rank or position to whom the data is to be disclosed*] 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

This notice may be verified by contacting the following:

[*enter contact details i.e. of the Single Point of Contact*]

Omit as appropriate

SCHEDULE 4

(Article 4)

CODE OF PRACTICE ON COVERT SURVEILLANCE

CONTENTS

Commencement

This code applies to every authorization of covert surveillance or of entry on or interference with property or with wireless telegraphy carried out under Part 11 of the Police Procedures and Criminal Evidence (Jersey) Law 2003 or Part 3 of the Regulation of Investigatory Powers (Jersey) Law 2005 by public authorities which begins on or after the day on which this code comes into effect.

1 BACKGROUND

1.1 In this code –

- "ECHR" means the European Convention on Human Rights;
- "PPCE" means the Police Procedures and Criminal Evidence (Jersey) Law 2003;
- "RIPL" means the Regulation of Investigatory Powers (Jersey) Law 2005.

1.2 This code of practice provides guidance on the use of covert surveillance by public authorities under Part 3 of RIPL and on entry on, or interference with, property (or with wireless telegraphy) under Part 11 of PPCE.

1.3 General observation forms part of the duties of many law enforcement officers and other public authorities and is not usually regulated by RIPL. For example, police officers while on patrol to prevent and detect crime, maintain public safety and prevent disorder may observe some suspicious activity or trading standards officers may covertly observe and visit a shop to verify the supply or level of supply of goods or services that may be liable to a restriction. Such observation may involve the use of equipment to merely reinforce normal sensory perception, such as binoculars, or the use of cameras, where this does not involve systematic surveillance of an individual.

1.4 Although, the provisions of RIPL or of this code of practice do not normally cover the use of overt CCTV surveillance systems, since members of the public are aware that such systems are in use, there may be occasions when public authorities use overt CCTV systems for the purposes of a specific investigation or operation. In such cases, authorization for intrusive or directed surveillance may be necessary.

1.5 RIPL provides that all codes of practice relating to the Law are admissible as evidence in criminal and civil proceedings. If any provision of the code appears relevant to any court or tribunal considering any such proceedings, or to the Tribunal established under the RIPL, or to the Commissioner responsible for overseeing the powers conferred by RIPL, it must be taken into account.

General extent of powers

1.6 Authorizations under RIPL can be given for surveillance both inside and outside Jersey. Authorizations for actions outside Jersey can only validate them for the purposes of proceedings in Jersey. An authorization under Part 2 of RIPL does not take into account the requirements of the country outside Jersey in which the investigation or operation is taking place.

Use of material in evidence

1.7 Material obtained through covert surveillance may be used as evidence in criminal proceedings. The proper authorization of surveillance should ensure the admissibility of such evidence under the customary law, Article 76 of PPCE and the Human Rights (Jersey) Law 2000. Furthermore, the product of the surveillance described in this code is subject to the ordinary rules for retention and disclosure of relevant unused material.

Directed surveillance, intrusive surveillance and entry on or interference with property or with wireless telegraphy

1.8 Directed surveillance is defined in Article 32(2) of RIPL as surveillance which is covert, but not intrusive, and undertaken:

(a) for the purposes of a specific investigation or specific operation;

(b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and

(c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be

reasonably practicable for an authorization under Part 3 of RIPL to be sought for the carrying out of the surveillance.

1.9 Directed surveillance investigations or operations can only be carried out by those public authorities who are listed in or added to Part 1 and Part 2 of Schedule 1 to RIPL.

1.10 Intrusive surveillance is defined in Article 32(3) of RIPL as covert surveillance that:

(a) is carried out in relation to anything taking place on any residential premises or in any private vehicle; and

(b) involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

1.11 Applications to carry out intrusive surveillance can only be granted by the Attorney General, an application made by one of the officers listed in Article 37(1) of RIPL or by a member or official to whom Article 37(7) of RIPL applies.

1.12 Applications to enter on or interfere with property or with wireless telegraphy can only be made to and granted by the Attorney General on an application by an official listed in Article 101(1A) of PPCE.

2 GENERAL RULES ON AUTHORIZATIONS

2.1 An authorization under Part 3 of RIPL will provide lawful authority for a public authority to carry out surveillance. Responsibility for authorizing surveillance investigations or operations will vary, depending on whether the authorization is for intrusive surveillance or directed surveillance, and which public authority is involved. For the purposes of Chapters 2 and 3 of this code the authorizing officer or the person who makes an application to the Attorney General will be referred to as an 'authorizing officer'.

2.2 Part 3 of RIPL does not impose a requirement on public authorities to seek or obtain an authorization where, under RIPL, one is available (see Article 57 of RIPL). Nevertheless, where there is an interference by a public authority with the right to respect for private and family life guaranteed under Article 8 of the ECHR, and where there is no other source of lawful authority, the consequence of not obtaining an authorization under RIPL may be that the action is unlawful by virtue of the Human Rights (Jersey) Law 2000.

2.3 Public authorities are therefore strongly recommended to seek an authorization where the surveillance is likely to interfere with a person's Article 8 rights to privacy by obtaining private information about that person, whether or not that person is the subject of the investigation or operation. Obtaining an authorization will ensure that the action is carried out in accordance with law and subject to stringent safeguards against abuse.

Necessity and Proportionality

2.4 Obtaining an authorization under RIPL or PPCE will only ensure that there is a justifiable interference with an individual's Article 8 rights if it

is necessary and proportionate for these activities to take place. RIPL first requires that the person granting an authorization believe that the authorization is necessary in the circumstances of the particular case for one or more of the statutory grounds in Article 34(3) of RIPL for directed surveillance and in Article 37(3) of RIPL for intrusive surveillance.

2.5 Then, if the activities are necessary, the person granting the authorization must believe that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

Collateral Intrusion

2.6 Before authorizing surveillance the authorizing officer should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (collateral intrusion). Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

2.7 An application for an authorization should include an assessment of the risk of any collateral intrusion. The authorizing officer should take this into account, when considering the proportionality of the surveillance.

2.8 Those carrying out the surveillance should inform the authorizing officer if the investigation or operation unexpectedly interferes with the privacy of individuals who are not covered by the authorization. When the original authorization may not be sufficient, consideration should be given to whether the authorization needs to be amended and reauthorized or a new authorization is required.

2.9 Any person granting or applying for an authorization or warrant will also need to be aware of particular sensitivities in the local community where the surveillance is taking place and of similar activities being undertaken by other public authorities which could impact on the deployment of surveillance. Where the authorizing officer is the Agent of the Impôts or the Chief Inspector of Immigration, he or she should consult a senior officer within the States of Jersey police.

2.10 The matters in paragraphs 2.1 - 2.9 must also be taken into account when applying for authorizations or warrants for entry on or interference with property or with wireless telegraphy. In particular they must be necessary in the circumstances of the particular case for one of the statutory ground listed Article 101(2)(a) of PPCE, proportionate and when exercised steps should be taken to minimise collateral intrusion.

Combined authorizations

2.11 A single authorization may combine:

- 2 or more different authorizations under Part 3 of RIPL;

- an authorization under Part 3 of RIPL and an authorization under Part 11 of PPCE.

2.12 For example, a single authorization may combine authorizations for directed and intrusive surveillance. The provisions applicable in the case of each of the authorizations must be considered separately. Thus, the Chief Officer of the States of Jersey Police can authorize the directed surveillance but the intrusive surveillance needs the separate authorization of the Attorney General. Where an authorization for directed surveillance or the use or conduct of a covert human intelligence source is combined with an Attorney General's authorization for intrusive surveillance, the combined authorization must be issued by the Attorney General. However, this does not preclude obtaining separate authorizations.

2.13 In cases where one agency is acting on behalf of another, it is usually for the tasking agency to obtain or provide the authorization. For example, where surveillance is carried out by the States Police on behalf of Customs or a Parish authority, authorizations would be sought by the police and granted by the Chief Officer. In a case where the Security Service is acting in support of the police or other law enforcement agency, in the field of serious crime, the Security Service would normally seek authorizations.

Central Record of all authorizations

2.14 A centrally retrievable record of all authorizations should be held by each public authority and regularly updated whenever an authorization is granted, renewed or cancelled. The record should be made available to the Commissioner upon request. These records should be retained for a period of at least 3 years from the ending of the authorization and should contain the following information:

- the type of authorization;
- the date the authorization was given;
- who gave the authorization;
- the unique reference number (URN) of the investigation or operation;
- the title of the investigation or operation, including a brief description and names of subjects, if known;
- whether the urgency provisions were used, and if so why.
- if the authorization is renewed, when it was renewed and who authorized the renewal, including the name and rank/grade of the authorizing officer;
- whether the investigation or operation is likely to result in obtaining confidential information as defined in this code of practice;
- the date the authorization was cancelled.

2.15 In all cases, the relevant authority should maintain the following documentation which need not form part of the centrally retrievable record:

- a copy of the application and a copy of the authorization together with any supplementary documentation and notification of the approval given by the authorizing officer;
- a record of the period over which the surveillance has taken place;
- the frequency of reviews prescribed by the authorizing officer;
- a record of the result of each review of the authorization;
- a copy of any renewal of an authorization, together with the supporting documentation submitted when the renewal was requested;
- the date and time when any instruction was given by the authorizing officer.

Retention and destruction of the product

2.16 Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable further period, commensurate to any subsequent review.

2.17 In the case of the law enforcement agencies particular attention is drawn to the requirements of customary law and the disclosures procedures in criminal proceedings. This requires that material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained.

2.18 There is nothing in RIPL which prevents material obtained from properly authorized surveillance from being used in other investigations. Each public authority must ensure that arrangements are in place for the handling, storage and destruction of material obtained through the use of covert surveillance. Authorizing officers must ensure compliance with the appropriate data protection requirements and any relevant codes of practice produced by individual authorities relating to the handling and storage of material.

The Intelligence Services, MOD and HM Forces

2.19 The heads of these agencies are responsible for ensuring that arrangements exist for securing that no information is stored by the authorities, except as necessary for the proper discharge of their functions. They are also responsible for arrangements to control onward disclosure.

3 SPECIAL RULES ON AUTHORIZATIONS

3.1 RIPL does not provide any special protection for 'confidential information'. Nevertheless, particular care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where confidential information is involved. Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material. So, for example, extra care should be given where, through the use of surveillance, it would be possible to acquire knowledge of discussions

between a minister of religion and an individual relating to the latter's spiritual welfare, or where matters of medical or journalistic confidentiality or legal privilege may be involved.

3.2 In cases where it is thought that through the use of surveillance, it is likely that confidential information will be acquired, it is recommended that advice is sought from the Law Officers' Department.

Communications Subject to Legal Privilege

3.3 Article 5 of PPCE describes those matters that are subject to legal privilege.

3.4 Legal privilege does not apply to communications made with the intention of furthering a criminal purpose (whether the lawyer is acting unwittingly or culpably). Legally privileged communications will lose their protection if there are grounds to believe, for example, that the professional legal adviser is intending to hold or use them for a criminal purpose. But privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence. The concept of legal privilege applies to the provision of professional legal advice by any individual, agency or organisation qualified to do so.

3.5 RIPL does not provide any special protection for legally privileged information. Nevertheless, such information is particularly sensitive and surveillance which acquires such material may engage Article 6 of the ECHR (right to a fair trial) as well as Article 8. Legally privileged information obtained by surveillance is extremely unlikely ever to be admissible as evidence in criminal proceedings. Moreover, the mere fact that such surveillance has taken place may lead to any related criminal proceedings being stayed as an abuse of process. Accordingly, action which may lead to such information being acquired is subject to additional safeguards under this code.

3.6 In general, an application for surveillance which is likely to result in the acquisition of legally privileged information should only be made in exceptional and compelling circumstances. Full regard should be had to the particular proportionality issues such surveillance raises. The application should include, in addition to the reasons why it is considered necessary for the surveillance to take place, an assessment of how likely it is that information subject to legal privilege will be acquired. In addition, the application should clearly state whether the purpose (or one of the purposes) of the surveillance is to obtain legally privileged information.

3.7 This assessment will be taken into account by the authorizing officer in deciding whether the proposed surveillance is necessary and proportionate under Article 34 of RIPL for directed surveillance and under Article 35 for intrusive surveillance. The authorizing officer may require regular reporting so as to be able to decide whether the authorization should continue. In those cases where legally privileged information has been acquired and retained, the matter should be reported to the Law Officers' Department and to the Commissioner during his or her next inspection and the material be made available to the Commissioner if requested.

3.8 A substantial proportion of the communications between a lawyer and his or her client(s) may be subject to legal privilege. Therefore, any case where a lawyer is the subject of an investigation or operation should be notified to the Commissioner and any material which has been retained should be made available to the Commissioner if requested.

3.9 Where there is any doubt as to the handling and dissemination of information which may be subject to legal privilege, advice should be sought from a legal adviser within the relevant public authority before any further dissemination of the material takes place. Similar advice should also be sought where there is doubt over whether information is not subject to legal privilege due to the "in furtherance of a criminal purpose" exception. The retention of legally privileged information, or its dissemination to an outside body, should be accompanied by a clear warning that it is subject to legal privilege. It should be safeguarded by taking reasonable steps to ensure there is no possibility of it becoming available, or its contents becoming known, to any person whose possession of it might prejudice any criminal or civil proceedings related to the information. Any dissemination of legally privileged material to an outside body should be notified to the Law Officers' Department and to the Commissioner during his or her next inspection.

Communications involving Confidential Personal Information and Confidential Journalistic Material

3.10 Similar consideration must also be given to authorizations that involve confidential personal information and confidential journalistic material. In those cases where confidential personal information and confidential journalistic material has been acquired and retained, the matter should be reported to the Law Officers' Department and to the Commissioner during his or her next inspection and the material be made available to the Commissioner if requested.

3.11 Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling concerning an individual (whether living or dead) who can be identified from it. Such information, which can include both oral and written communications, is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. Examples might include consultations between a health professional and a patient, or information from a patient's medical records.

3.12 Spiritual counselling means conversations between an individual and a Minister of Religion acting in his or her official capacity, where the individual being counselled is seeking or the Minister is imparting forgiveness, absolution or the resolution of conscience with the authority of the Divine Being(s) of their faith.

3.13 Confidential journalistic material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information

being acquired for the purposes of journalism and held subject to such an undertaking.

4 AUTHORIZATION PROCEDURES FOR DIRECTED SURVEILLANCE

4.1 Directed surveillance is defined in Article 32(1) of RIPL as surveillance which is covert, but not intrusive, and undertaken:

(a) for the purposes of a specific investigation or specific operation;

(b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and

(c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorization under Part 3 of RIPL to be sought for the carrying out of the surveillance.

4.2 Covert surveillance is defined in Article 32(8)(a) of RIPL as any surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place.

4.3 Private information is defined in Article 32(9) of RIPL as including any information relating to a person's private or family life. The concept of private information should be broadly interpreted to include an individual's private or personal relationship with others. Family life should be treated as extending beyond the formal relationships created by marriage.

4.4 Directed surveillance does not include covert surveillance carried out by way of an immediate response to events or circumstances which, by their very nature, could not have been foreseen. For example, a police officer would not require an authorization to conceal himself or herself and observe a suspicious person that the officer came across in the course of a patrol.

4.5 By virtue of Article 31(3) of RIPL, surveillance includes the interception of postal and telephone communications where the sender or recipient consents to the reading of or listening to or recording of the communication (as the case may be). For further details see paragraphs 4.30 - 4.32 of this code.

4.6 Surveillance in residential premises or in private vehicles is defined as intrusive surveillance in Article 32(2) of RIPL and is dealt with in Chapter 5 of this code. However, where surveillance is carried out by a device designed or adapted principally for the purpose of providing information about the location of a vehicle, the activity is directed surveillance and should be authorized accordingly.

4.7 Directed surveillance does not include entry on or interference with property or with wireless telegraphy. These activities are subject to a separate regime of authorization or warranty, as set out in Chapter 6 of this code.

4.8 Directed surveillance includes covert surveillance within office premises, (as defined in paragraph 6.31 of this code). Authorizing officers are

reminded that confidential information should be afforded an enhanced level of protection.

Authorization Procedures

4.9 Under Article 34(3) of RIPL an authorization for directed surveillance may be granted by a "designated person" (the authorizing officer) where he or she believes that the authorization is necessary in the circumstances of the particular case:

- in the interests of national security[7],[8];
- for the purpose of preventing and detecting[9] crime or of preventing disorder;
- in the interests of the economic well-being of Jersey;
- in the interests of public safety;
- for the purpose of protecting public health[10];
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or
- for any other purpose prescribed by an Order made by the Minister for Home Affairs.[11]

4.10 The authorizing officer must also believe that the surveillance is proportionate to what it seeks to achieve.

4.11 The public authorities entitled to apply for and the authorizing officers entitled to authorize directed surveillance are listed in Schedule 2 to RIPL. Responsibility for authorizing the carrying out of directed surveillance rests with the authorizing officer and requires the personal authority of the authorizing officer. Where an authorization for directed surveillance is combined with an Attorney General's authorization for intrusive surveillance, the combined authorization must be issued by the Attorney General.

4.12 The authorizing officer must give authorizations in writing, except that in urgent cases, they may be given orally by the authorizing officer. In such cases, a statement that the authorizing officer has expressly authorized the

[7] One of the functions of the Security Service is the protection of national security and in particular the protection against threats from terrorism. These functions extend throughout the British Isles.

[8] HM Forces may also undertake operations in connection with a military threat to national security and other operations in connection with national security and other operations in connection with national security in support of the Security Service, or other Civil Powers.

[9] "Detecting crime" is defined in Article 1(2) of RIPL and is applied to Article 101 of PPCE.

[10] This could include investigations into infectious diseases, contaminated products or the illicit sale of pharmaceuticals.

[11] This could only be for a purpose which satisfied the criteria set out in Article 8(2) of the ECHR.

action should be recorded in writing by the applicant as soon as is reasonably practicable.

4.13 A case is not normally to be regarded as urgent unless the time that would elapse before the authorizing officer was available to grant the authorization would, in the judgement of the person giving the authorization, be likely to endanger life or jeopardise the investigation or operation for which the authorization was being given. An authorization is not to be regarded as urgent where the need for an authorization has been neglected or the urgency is of the authorizing officer's own making.

4.14 Authorizing officers should not be responsible for authorizing investigations or operations in which they are directly involved, although it is recognized that this may sometimes be unavoidable, especially in the case of small organizations. Where an authorizing officer authorizes such an investigation or operation the central record of authorizations (see paragraphs 2.14 -2.15) should highlight this and the attention of the Commissioner should be invited to it.

4.15 Authorizing officers within the Police, Customs and Immigration may only grant authorizations on application by a member of the force or their Department as the case may be.

Information to be provided in applications for authorization

4.16 A written application for authorization for directed surveillance should describe any conduct to be authorized and the purpose of the investigation or operation. The application should also include:

- the reasons why the authorization is necessary in the particular case and on the grounds (*e.g.* for the purpose of preventing or detecting crime) listed in Article 34(3) of RIPL;
- the reasons why the surveillance is considered proportionate to what it seeks to achieve;
- the nature of the surveillance;
- the identities, where known, of those to be the subject of the surveillance;
- an explanation of the information which it is desired to obtain as a result of the surveillance;
- the details of any potential collateral intrusion and why the intrusion is justified;
- the details of any confidential information that is likely to be obtained as a consequence of the surveillance.
- the level of authority required (or recommended where that is different) for the surveillance; and
- a subsequent record of whether authority was given or refused, by whom and the time and date.

4.17 Additionally, in urgent cases, the authorization should record (as the case may be) the reasons why it was not reasonably practicable for the application to be considered by the authorizing officer and the reasons why the authorizing officer or the officer entitled to act in urgent cases

considered the case so urgent that an oral instead of a written authorization was given; and/or

4.18 Where the authorization is oral, the detail referred to above should be recorded in writing by the applicant as soon as reasonably practicable.

Duration of authorizations

4.19 A written authorization granted by an authorizing officer will cease to have effect (unless renewed) at the end of a period of 3 months beginning with the day on which it took effect.

4.20 Urgent oral authorizations or written authorizations granted by a person who is entitled to act only in urgent cases will, unless renewed, cease to have effect after 72 hours, beginning with the time when the authorization was granted or renewed.

Reviews

4.21 Regular reviews of authorizations should be undertaken to assess the need for the surveillance to continue. The results of a review should be recorded on the central record of authorizations (see paragraphs 2.14 - 2.15). Particular attention is drawn to the need to review authorizations frequently where the surveillance provides access to confidential information or involves collateral intrusion.

4.22 In each case the authorizing officer within each public authority should determine how often a review should take place. This should be as frequently as is considered necessary and practicable.

Renewals

4.23 If at any time before an authorization would cease to have effect, the authorizing officer considers it necessary for the authorization to continue for the purpose for which it was given, he may renew it in writing for a further period of 3 months. Renewals may also be granted orally in urgent cases and last for a period of 72 hours.

4.24 A renewal takes effect at the time at which, or day on which the authorization would have ceased to have effect but for the renewal. An application for renewal should not be made until shortly before the authorization period is drawing to an end. Any person who would be entitled to grant a new authorization can renew an authorization. Authorizations may be renewed more than once, provided they continue to meet the criteria for authorization.

4.25 All applications for the renewal of an authorization for directed surveillance should record:

- whether this is the first renewal or every occasion on which the authorization has been renewed previously;
- any significant changes to the information in paragraph 4.16;
- the reasons why it is necessary to continue with the directed surveillance;
- the content and value to the investigation or operation of the information so far obtained by the surveillance;

- the results of regular reviews of the investigation or operation.

4.26 Authorizations may be renewed more than once, if necessary, and the renewal should be kept/recorded as part of the central record of authorizations (see paragraphs 2.14 - 2.15).

Cancellations

4.27 The authorizing officer who granted or last renewed the authorization (or his or her deputy) must cancel it if the officer is satisfied that the directed surveillance no longer meets the criteria upon which it was authorized. Where the authorizing officer is no longer available, this duty will fall on the person who is acting as authorizing officer or has taken over the rôle of authorizing officer.

Ceasing of surveillance activity

4.28 As soon as the decision is taken that directed surveillance should be discontinued, the instruction must be given to those involved to stop all surveillance of the subject(s). The date and time when such an instruction was given should be recorded in the central record of authorizations (see paragraphs 2.14 - 2.15) and the notification of cancellation where relevant.

ADDITIONAL RULES

Recording of telephone conversations

4.29 Subject to paragraph 4.30, the interception of communications sent by post or by means of public telecommunications systems or private telecommunications systems attached to the public network may be authorized only by the Attorney General, in accordance with the terms of Part 1 of RIPL. Nothing in this code should be taken as granting dispensation from the requirements of that Part of RIPL.

4.30 Part 2 of RIPL provides certain exceptions to the rule that interception of telephone conversations must be warranted under that Part. This includes the situation in which one party to the communication consents to the interception, it may be authorized in accordance with Article 31(3) of RIPL provided that there is no interception warrant authorizing the interception. In such cases, the interception is treated as directed surveillance.

4.31 The use of a surveillance device should not be ruled out simply because it may incidentally pick up one or both ends of a telephone conversation, and any such product can be treated as having been lawfully obtained. However, its use would not be appropriate where the sole purpose is to overhear speech which, at the time of monitoring, is being transmitted by a telecommunications system. In such cases an application should be made for an interception of communication warrant under Article 10 of RIPL.

5 AUTHORIZATION PROCEDURES FOR INTRUSIVE SURVEILLANCE

5.1 Intrusive surveillance is define in Article 32(2) of RIPL as covert surveillance that:

(a) is carried out in relation to anything taking place on any residential premises or in any private vehicle; and

(b) involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

5.2 Covert surveillance is defined in Article 32(9)(a) of RIPL as any surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place.

5.3 Where surveillance is carried out in relation to anything taking place on any residential premises or in any private vehicle by means of a device, without that device being present on the premises, or in the vehicle, it is not intrusive unless the device consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle. Thus, an observation post outside premises, which provides a limited view and no sound of what is happening inside the premises would not be considered as intrusive surveillance.

5.4 Residential premises are defined in Article 30(1) of RIPL. The definition includes hotel rooms, bedrooms in barracks, and police and prison cells but not any common area to which a person is allowed access in connection with his or her occupation of such accommodation *e.g.* a hotel lounge.

5.5 A private vehicle is defined in Article 30(1) of RIPL as any vehicle which is used primarily for the private purposes of the person who owns it or of a person otherwise having the right to use it. A person does not have a right to use a motor vehicle if his or her right to use it derives only from the person's having paid, or undertaken to pay, for the use of the vehicle and its driver for a particular journey.

5.6 In many cases, a surveillance investigation or operation may involve both intrusive surveillance and entry on or interference with property or with wireless telegraphy. In such cases, both activities need authorization. This can be done as a combined authorization (see paragraph 2.11).

5.7 An authorization for intrusive surveillance may be issued by the Attorney General.

5.8 All authorizations require the personal authority of the Attorney General. Any members or officials of the intelligence services, the Ministry of Defence and HM Forces can apply to the Attorney General for an intrusive surveillance warrant. Under Article 37(2) of RIPL the Attorney General may not authorize intrusive surveillance unless he or she believes –

(a) that the authorization is necessary in the circumstances of the particular case on the grounds that it is:

- in the interests of national security;
- for the purpose of preventing or detecting serious crime; or
- in the interests of the economic well-being of Jersey;

and

(b) that the surveillance is proportionate to what it seeks to achieve.

5.9 A factor which must be taken into account in deciding whether an authorization is necessary and proportionate is whether the information which it is thought necessary to obtain by means of the intrusive surveillance could reasonably be obtained by other less intrusive means.

Authorizations Procedures for Police, Customs and Excise and Immigration

5.10 The Attorney General will generally give authorizations in writing. However, in urgent cases, they may be given orally. In an urgent oral case, a statement that the Attorney General has expressly authorized the conduct should be recorded in writing by the applicant as soon as is reasonably practicable.

5.11 A case is not normally to be regarded as urgent unless the time that would elapse before the Attorney General was available to grant the authorization would, in the judgement of the person giving the authorization, be likely to endanger life or jeopardise the investigation or operation for which the authorization was being given. An authorization is not to be regarded as urgent where the need for an authorization has been neglected or the urgency is of the authorizing officer's own making.

5.12 Applications should be in writing and describe the conduct to be authorized and the purpose of the investigation or operation. The application should specify:

- the reasons why the authorization is necessary in the particular case and on the grounds (*e.g.* for the purpose of preventing or detecting serious crime) listed in Article 37(3) of RIPL;
- the reasons why the surveillance is considered proportionate to what it seeks to achieve;
- the nature of the surveillance;
- the residential premises or private vehicle in relation to which the surveillance will take place;
- the identities, where known, of those to be the subject of the surveillance;
- an explanation of the information which it is desired to obtain as a result of the surveillance;
- details of any potential collateral intrusion and why the intrusion is justified;
- details of any confidential information that is likely to be obtained as a consequence of the surveillance.
- a subsequent record should be made of whether authority was given or refused, and the time and date.

5.13 Additionally, in urgent cases, the authorization should record the reasons why the Attorney General considered the case so urgent that an oral instead of a written authorization was given.

5.14 Where the application is oral, the detail referred to above should be recorded in writing as soon as reasonably practicable.

Notifications to Investigatory Powers Commissioner

5.15 The Attorney General must give notice in writing, at least every 12 months, of the grant, renewal or cancellation of an authorization to the Commissioner, in accordance with whatever arrangements have been made by the Commissioner.

5.16 In respect of urgent cases, the notification must specify the grounds on which the case was believed to be one of urgency. The urgency provisions should not be used routinely.

All intrusive surveillance authorizations

5.17 Paragraphs 5.18 to 5.27 deal with the duration, renewal and cancellation of authorizations. Unless otherwise specified the guidance below applies to all authorizations.

Duration of Authorizations

5.18 A written authorization granted by the Attorney General, will cease to have effect (unless renewed) at the end of a period of **3 months**, beginning with the day on which it took effect.

5.19 Oral authorizations given in urgent cases by the Attorney General will cease to have effect (unless renewed) at the end of the period of **72** hours beginning with the time when they took effect.

Attorney General's intelligence services authorizations

5.20 A warrant issued by the Attorney General will cease to have effect at the end of a period of 3 months beginning with the day on which it was issued.

Renewals

5.21 If at any time before an authorization expires the Attorney General considers the authorization should continue to have effect for the purpose for which it was issued, the Attorney General may renew it in writing for a further period of **3 months**.

5.22 Subject to paragraph 5.36, if at any time before the day on which the Attorney General's authorization expires, the Attorney General considers it necessary for the warrant to be renewed for the purpose for which it was issued, he or she may renew it in writing for a further period of 3 months, beginning with the day on which it would have ceased to have effect, but for the renewal.

Intelligence services authorizations

5.23 **All applications** for a renewal of an authorization or warrant should record:

- whether this is the first renewal or every occasion on which the warrant/authorization has been renewed previously;
- any significant changes to the information listed in paragraph 5.12;
- the reasons why it is necessary to continue with the intrusive surveillance;

- the content and value to the investigation or operation of the product so far obtained by the surveillance;
- the results of regular reviews of the investigation or operation.

5.24 Authorizations may be renewed more than once, if necessary, and the renewal should be kept/recorded as part of the central record of authorizations (see paragraphs 2.14 - 2.15).

Reviews

5.25 Regular reviews of authorizations should be undertaken to assess the need for the surveillance to continue. The results of a review should be recorded on the central record of authorizations (see paragraphs 2.14 - 2.15). Particular attention is drawn to the need to review authorizations frequently where the intrusive surveillance provides access to confidential information or involves collateral intrusion.

5.26 The member or official who made the application to the Attorney General should determine how often a review should take place. This should be as frequently as is considered necessary and practicable.

Cancellations

5.27 The Attorney General shall cancel an authorization if he or she is satisfied that the surveillance no longer meets the criteria upon which it was authorized.

Ceasing of surveillance activity

5.28 As soon as the decision is taken that the intrusive surveillance should be discontinued, instructions must be given to those involved to stop all surveillance of the subject(s). The date and time when such an instruction was given should be recorded in the central record of authorizations (see paragraphs 2.14 - 2.15) and the notification of cancellation where relevant.

6 AUTHORIZATION PROCEDURES FOR ENTRY ON OR INTERFERENCE WITH PROPERTY OR WITH WIRELESS TELEGRAPHY

6.1 Part 11 of PPCE provides lawful authority for entry on or interference with property or with wireless telegraphy by the police, intelligence services, customs and excise, and immigration.

6.2 In many cases a covert surveillance operation may involve both intrusive surveillance and entry on or interference with property or with wireless telegraphy. This can be done as a combined authorization, although the criteria for authorization of each activity must be considered separately (see paragraph 2.11).

Authorizations for entry on or interference with property or with wireless telegraphy by the police, Customs and Immigration

6.3 Responsibility for such authorizations rests with the Attorney General.

6.4 Authorizations under PPCE may not be necessary where the public authority is acting with the consent of a person able to give permission in

respect of relevant property, although consideration should still be given to the need to obtain an authorization under Part 3 of RIPL.

6.5 In giving an authorization for entry on or interference with property or with wireless telegraphy under Article 101(2) of PPCE, the Attorney General must believe that:

- it is necessary for the action specified to be taken for the purpose of preventing or detecting serious crime in the interests of national security; and
- that the taking of the action is proportionate to what the action seeks to achieve.

6.6 The Attorney General must take into account whether what it is thought necessary to achieve by the authorized conduct could reasonably be achieved by other means.

6.7 Any person applying for an authorization or warrant to enter on or interfere with property or with wireless telegraphy will also need to be aware of particular sensitivities in the local community where the entry or interference is taking place and of similar activities being undertaken by other public authorities which could impact on the deployment.

Authorization procedures for entry on or interference with property or with wireless telegraphy by the police, Customs and Immigration

6.8 Authorizations will be given in writing by the Attorney General. However, in urgent cases, they may be given orally. In such cases, a statement that the Attorney General has expressly authorized the action should be recorded in writing by the applicant as soon as is reasonably practicable. This should be done by the person with whom the Attorney General spoke.

6.9 Applications to the Attorney General for authorization must be made in writing by the Chief Officer, Agent of the Impôts or Chief Inspector of Immigration and should specify:

- the identity or identities of those to be targeted (where known);
- the property which the entry or interference with will affect;
- the identity of individuals and/or categories of people, where known, who are likely to be affected by collateral intrusion;
- details of the offence planned or committed;
- details of the intrusive surveillance involved;
- how the authorization criteria (as set out in paragraphs 6.6 and 6.7) have been met;
- any action which may be necessary to retrieve any equipment used in the surveillance;
- in case of a renewal, the results obtained so far, or a full explanation of the failure to obtain any results; and
- whether an authorization was given or refused, by whom and the time and date.

6.10 Additionally, in urgent cases, the authorization should record the reasons why the applying officer considered the case so urgent that an oral instead of a written authorization was given.

6.11 Where the application is oral, the information referred to above should be recorded in writing by the applicant as soon as reasonably practicable.

Notifications to Surveillance Commissioners

6.12 The Attorney General must give notice in writing when he or she grants, renews or cancels an authorization to the Commissioner, at least every 12 months, in accordance with arrangements made by the Commissioner.

Duration of authorizations

6.13 Written authorizations will cease to have effect at the end of a period of 3 months beginning with the day on which they took effect.

6.14 Oral authorizations given in urgent cases will cease at the end of the period of **72** hours beginning with the time when they took effect.

Renewals

6.15 If at any time before the day on which an authorization expires the Attorney General considers the authorization should continue to have effect for the purpose for which it was issued, the Attorney General may renew it in writing for a period of 3 months beginning with the day on which the authorization would otherwise have ceased to have effect. Authorizations may be renewed more than once, if necessary, and the renewal should be recorded on the authorization record (see paragraph 6.27).

6.16 The Commissioner must be notified of renewals of authorizations.

Reviews

6.17 The Attorney General should ensure regular reviews are made of authorizations, to assess the need for the entry on or interference with property or with wireless telegraphy to continue. This should be recorded on the authorization record (see paragraph 6.27). The Attorney General should determine how often a review should take place when giving an authorization and who should undertake it. This can be delegated to a senior officer of the authority that made the application. This should be as frequently as is considered necessary and practicable and at no greater interval than one month. Particular attention is drawn to the need to review authorizations and renewals regularly and frequently where the entry on or interference with property or with wireless telegraphy provides access to confidential information or involves collateral intrusion.

Cancellations

6.18 The Attorney General must cancel an authorization, or the person who made the application to the Attorney General must apply for its cancellation, if he or she is satisfied that the authorization no longer meets the criteria upon which it was authorized.

6.19 The Commissioner must be notified of cancellations of authorizations.

6.20 The Tribunal has the power to cancel an authorization if satisfied that, at any time after an authorization was given or renewed, there were no reasonable grounds for believing the matters set out in paragraphs 6.5 and 6.6. In such circumstances, the Tribunal may order the destruction of records, in whole or in part, other than any that are required for pending criminal or civil proceedings.

Authorization record

6.21 An authorization record should be created which records:

- the time and date when an authorization is given;
- whether an authorization is in written or oral form;
- the time and date when it was notified to the Commissioner;

The authorization record should also record:

- every occasion when entry on or interference with property or with wireless telegraphy has occurred;
- the result of periodic reviews of the authorization;
- the date of every renewal; and
- it should record the time and date when any instruction was given by the authorizing officer to cease the interference with property or with wireless telegraphy.

Ceasing of entry on or interference with property or with wireless telegraphy

6.22 Once an authorization or renewal expires or is cancelled or quashed, the Attorney General must immediately instruct those carrying out the surveillance to cease all the actions authorized for the entry on or interference with property or with wireless telegraphy. The time and date when such an instruction was given should be recorded on the authorization record (see paragraph 6.21).

Retrieval of equipment

6.23 Where the Tribunal quashes, or cancels, an authorization or renewal, it will, if there are reasonable grounds for doing so, order that the authorization remain effective for a specified period, to enable officers to retrieve anything left on the property by virtue of the authorization. It can only do so if the authorization or renewal makes provision for this.

Special situations

6.24 In certain cases, special care must be used in considering or granting an authorization for entry on or interference with property (pursuant to Part 11 of PPCE). These are cases where it is believed that:

- any of the property specified in the authorization:
  - is used wholly or mainly as a dwelling or a bedroom in a hotel; or
  - constitutes office premises; or
- the action authorized is likely to result in any person acquiring knowledge of:

- matters subject to legal privilege;
- confidential personal information; or
- confidential journalistic material.

6.25 Office premises are defined as any building or part of a building whose sole or principal use is as an office or for office purposes (which means purposes of administration, clerical work, handling money and telephone or telegraphic operation).

Authorizations for entry on or interference with property or with wireless telegraphy by the intelligence services

6.26 Before granting a warrant, the Attorney General must:

- think it necessary for the action to be taken for the purpose of assisting the relevant agency in carrying out its functions;
- be satisfied that the taking of the action is proportionate to what the action seeks to achieve;
- take into account in deciding whether an authorization is necessary and proportionate is whether the information which it is thought necessary to obtain by the conduct authorized by the warrant could reasonably be obtained by other means.

6.27 An application for a warrant must be made by a member of the intelligence services for the taking of action in relation to that agency. In addition, the Security Service may make an application for a warrant to act on behalf of the Secret Intelligence Service (SIS) and the Governments Communication Headquarters (GCHQ). SIS and GCHQ may not be granted a warrant for action in support of the prevention or detection of serious crime which relates to property in Jersey.

6.28 A warrant shall, unless renewed, cease to have effect at the end of the period of **3 months** beginning with the day on which it was issued. In any other case, at the end of the period ending with the **second working day** following that day.

6.29 If at any time before the day on which a warrant would cease to have effect the Attorney General considers it necessary for the warrant to continue to have effect for the purpose for which it was issued, the Attorney General may by an instrument under his or her hand renew it for a period of **3 months** beginning with that day. The Attorney General shall cancel a warrant if he or she is satisfied that the action authorized by it is no longer necessary.

6.30 The intelligence services should provide the same information as the police, as and where appropriate, when making applications, requests for renewal and requests for cancellation of property warrants.

Retrieval of equipment

6.31 Because of the time it can take to remove equipment from a person's property it may also be necessary to renew a property warrant in order to complete the retrieval. Applications to the Attorney General for renewal should state why it is being or has been closed down, why it has not been possible to remove the equipment and any timescales for removal, where known.

7 OVERSIGHT BY COMMISSIONERS

7.1 PPCE and RIPL require the Commissioner to keep under review (with the assistance of the Assistant Commissioners) the performance of functions under Part 11 PPCE and Part 3 of RIPL.

7.2 This code does not cover the exercise of any of the Commissioners' functions. It is the duty of any person who uses these powers to comply with any request made by a Commissioner to disclose or provide any information the Commissioner requires for the purpose of enabling the Commissioner to carry out his or her functions.

7.3 References in this code to the performance of review functions by the Commissioner apply also to any Inspectors and other members of staff to whom such functions have been delegated.

8 COMPLAINTS

8.1 RIPL establishes an independent Tribunal. This Tribunal will be made up of a judge of the Court of Appeal and 2 Jurats and is independent of the States. The Tribunal has powers to investigate and decide any case within its jurisdiction.

This code does not cover the exercise of the Tribunal's functions. Details of the relevant complaints procedure can be obtained from the following address:

Judicial Greffier

Morier House

St Helier

Jersey

JE1 1DD

SCHEDULE 5

(Article 5)

CODE OF PRACTICE ON COVERT HUMAN INTELLIGENCE SOURCES

CONTENTS

Commencement

This code applies to every authorization of the use or conduct by public authorities of covert human intelligence sources carried out under Part 3 of the Regulation of Investigatory Powers (Jersey) Law 2005 which begins on or after the day on which this code comes into effect.

1 BACKGROUND - GENERAL - COMMENCEMENT

1.1 In this code –

- "**ECHR**" means the European Convention on Human Rights;
- **"PPCE"** means the Police Procedures and Criminal Evidence (Jersey) Law 2003;
- **"Law"** means the Regulation of Investigatory Powers (Jersey) Law 2005;

1.2 This Code of practice provides guidance on the authorization of the use or conduct of covert human intelligence sources ("a source") by public authorities under Part 3 of the Law and it applies to every such authorization or the use or conduct by 3 public authorities of covert human intelligence sources carried out under the Law which begins on or after the day on which this Code comes into effect.

1.3 The provisions of the Law are not intended to apply in circumstances where members of the public volunteer information to the police or other authorities, as part of their normal civic duties, or to contact numbers set up to receive information (such as Crimestoppers, Customs Confidential, the Anti Terrorist Hotline, or the Security Service Public Telephone

Number). Members of the public acting in this way would not generally be regarded as sources.

1.4 Neither Part 3 of the Law or this code of practice is intended to affect the practices and procedures surrounding criminal participation of sources.

1.5 The Law provides that all codes of practice relating to the Law are admissible as evidence in criminal and civil proceedings. If any provision of the code appears relevant to any court or tribunal considering any such proceedings, or to the Investigatory Powers Tribunal established under the Law, or to the Commissioner responsible for overseeing the powers conferred by the Law, it must be taken into account.

General extent of powers

1.6 Authorizations can be given for the use or conduct of a source both inside and outside Jersey. Authorizations for actions outside Jersey can only validate them for the purposes of proceedings in Jersey. An authorization under Part 3 of the Law does not take into account the requirements of the country outside Jersey in which the investigation or operation is taking place.

1.7 Members of foreign law enforcement or other agencies or sources of those agencies may be authorized under the Law in Jersey in support of domestic and international investigations.

Use of material in evidence

1.8 Material obtained from a source may be used as evidence in criminal proceedings. The proper authorization of a source should ensure the suitability of such evidence under the customary law, Article 76 of PPCE and the Human Rights (Jersey) Law 2000. Furthermore, the product obtained by a source described in this code is subject to the ordinary rules for retention and disclosure of material, where those rules apply to the law enforcement body in question. There are also well-established legal procedures that will protect the identity of a source from disclosure in such circumstances.

2 GENERAL RULES ON AUTHORIZATIONS

2.1 An authorization under Part 3 of the Law will provide lawful authority for the use of a source. Responsibility for giving the authorization will depend on which public authority is responsible for the source.

2.2 Part 3 of the Law does not impose a requirement on public authorities to seek or obtain an authorization where, under the Law, one is available (see Article 57 of the Law). Nevertheless, where there is an interference by a public authority with the right to respect for private and family life guaranteed under Article 8 of the ECHR, and where there is no other lawful authority, the consequences of not obtaining an authorization under the Law may be that the action is unlawful by virtue of Article 7 of the Human Rights (Jersey) Law 2000.

2.3 Public authorities are therefore strongly recommended to seek an authorization where the use or conduct of a source is likely to interfere

with a person's Article 8 rights to privacy by obtaining information from or about a person, whether or not that person is the subject of the investigation or operation. Obtaining an authorization will ensure that the action is carried out in accordance with law and subject to stringent safeguards against abuse.

Necessity and Proportionality

2.4 Obtaining an authorization under the Law will only ensure that the authorized use or conduct of a source is a justifiable interference with an individual's Article 8 rights if it is necessary and proportionate for the source to be used. The Law first requires that the person granting an authorization must believe that the authorization is necessary in the circumstances of the particular case for one or more of the statutory grounds in Article 35(3) of the Law.

2.5 Then, if the use of the source is necessary, the person granting the authorization must believe that the use of a source is proportionate to what is sought to be achieved by the conduct and use of that source. This involves balancing the intrusiveness of the use of the source on the target and others who might be affected by it against the need for the source to be used in operational terms. The use of a source will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. The use of a source should be carefully managed to meet the objective in question and sources must not be used in an arbitrary or unfair way.

Collateral Intrusion

2.6 Before authorizing the use or conduct of a source, the authorizing officer should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the operation or investigation (collateral intrusion). Measures should be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those not directly connected with the operation.

2.7 An application for an authorization should include an assessment of the risk of any collateral intrusion. The authorizing officer should take this into account, when considering the proportionality of the use and conduct of a source.

2.8 Those tasking a source should inform the authorizing officer if the investigation or operation unexpectedly interferes with the privacy of individuals who are not covered by the authorization. When the original authorization may not be sufficient, consideration should be given to whether the authorization needs to be amended and reauthorized or a new authorization is required.

2.9 Any person granting or applying for an authorization will also need to be aware of any particular sensitivities in the local community where the source is being used and of similar activities being undertaken by other public authorities which could impact on the deployment of the source. Consideration should also be given to any adverse impact on community confidence or safety that may result from the use or conduct of a source or of information obtained from that source. Additionally, the authorizing

officer should make an assessment of any risk to a source in carrying out the proposed authorization.

2.10 In a very limited range of circumstances an authorization under Part 3 may, by virtue of Articles 32(6) and 33 of the Law, render lawful conduct which would otherwise be criminal, if it is incidental to any conduct falling within Article 32(7) of the Law which the source is authorized to undertake. This would depend on the circumstances of each individual case, and consideration should always be given to seeking advice from the Law Officers' Department when such activity is contemplated. A source that acts beyond the limits recognised by the law will be at risk from prosecution. The need to protect the source cannot alter this principle.

Combined authorizations

2.11 A single authorization may combine 2 or more different authorizations under Part 3 of the Law. For example, a single authorization may combine authorizations for intrusive surveillance and the conduct of a source. In such cases the provisions applicable to each of the authorizations must be considered separately. Thus, the Chief Officer of the Force can authorize the conduct of a source but an authorization for intrusive surveillance by the police needs the separate authority of the Attorney General. Where an authorization for the use or conduct of a covert human intelligence source is combined with the Attorney General's authorization for intrusive surveillance, the combined authorization must be issued by the Attorney General. However, this does not preclude public authorities from obtaining separate authorizations.

Directed surveillance against a potential source

2.12 It may be necessary to deploy directed surveillance against a potential source as part of the process of assessing their suitability for recruitment, or in planning how best to make the approach to them. An authorization under this code authorizing an officer to establish a covert relationship with a potential source could be combined with a directed surveillance authorization so that both the officer and potential source could be followed. Directed surveillance is defined in Article 32(1) of the Law. See the code of practice on Covert Surveillance.

Central Record of all authorizations

2.13 A centrally retrievable record of all authorizations should be held by each public authority and regularly updated whenever an authorization is granted, renewed or cancelled. The record should be made available to the Commissioner or an Inspector from the Office of Commissioner, upon request. These records should be retained for a period of at least 3 years from the ending of the authorization.

2.14 Proper records must be kept of the authorization and use of a source. Article 35(5) of the Law provides that an authorizing officer must not grant an authorization for the use or conduct of a source unless he or she believes that there are arrangements in place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the source.

2.15 In addition, records or copies of the following, as appropriate, should be kept by the relevant authority:

- a copy of the authorization together with any supplementary documentation and notification of the approval given by the authorizing officer;
- a copy of any renewal of an authorization, together with the supporting documentation submitted when the renewal was requested;
- the reason why the person renewing an authorization considered it necessary to do so;
- any authorization which was granted or renewed orally (in an urgent case) and the reason why the case was considered urgent;
- any risk assessment made in relation to the source;
- the circumstances in which tasks were given to the source;
- the value of the source to the investigating authority;
- a record of the results of any reviews of the authorization;
- the reasons, if any, for not renewing an authorization;
- the reasons for cancelling an authorization.
- the date and time when any instruction was given by the authorizing officer to cease using a source.

2.16 The records kept by public authorities should be maintained in such a way as to preserve the confidentiality of the source and the information provided by that source. There should, at all times, be a designated person within the relevant public authority who will have responsibility for maintaining a record of the use made of the source.

Retention and destruction of the product

2.17 Where the product obtained from a source could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable further period, commensurate to any subsequent review.

2.18 In the cases of the law enforcement agencies, particular attention is drawn to the requirements that material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained.

2.19 There is nothing in the Law which prevents material obtained from properly authorized use of a source being used in other investigations. Each public authority must ensure that arrangements are in place for the handling, storage and destruction of material obtained through the use of a source. Authorizing officers must ensure compliance with the appropriate data protection requirements and any relevant codes of practice produced by individual authorities in the handling and storage of material.

3 SPECIAL RULES ON AUTHORIZATIONS

Confidential Information

3.1 The Law does not provide any special protection for 'confidential information'. Nevertheless, particular care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where confidential information is involved. Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material.

3.2 In cases where, through the use of or conduct of a source, it is likely that knowledge of confidential information will be acquired, it is recommended that the grant of authority to deploy the source is considered at a senior level and, in case of difficulty, advice sought from the Law Officers' Department.

Communications Subject to Legal Privilege

3.3 Article 5 of PPCE describes those matters that are subject to legal privilege.

3.4 Legal privilege does not apply to communications made with the intention of furthering a criminal purpose (whether the lawyer is acting unwittingly or culpably). Legally privileged communications will lose their protection if there are grounds to believe, for example, that the professional legal adviser is intending to hold or use them for a criminal purpose. But privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence. The concept of legal privilege applies to the provision of professional legal advice by any individual, agency or organisation qualified to do so.

3.5 The Law does not provide any special protection for legally privileged information. Nevertheless, such information is particularly sensitive and any source which acquires such material may engage Article 6 of the ECHR (right to a fair trial) as well as Article 8. Legally privileged information obtained by a source is extremely unlikely ever to be admissible as evidence in criminal proceedings. Moreover, the mere fact that use has been made of a source to obtain such information may lead to any related criminal proceedings being stayed as an abuse of process. Accordingly, action which may lead to such information being obtained is subject to additional safeguards under this code.

3.6 In general, an application for the use or conduct of a source which is likely to result in the acquisition of legally privileged information should only be made in exceptional and compelling circumstance. Full regard should be had to the particular proportionality issues such a use or conduct of a source raises. The application should include, in addition to the reasons why it is considered necessary for the use or conduct of a source to be used, an assessment of how likely it is that information subject to legal privilege will be acquired. The application should clearly state whether the purpose (or one of the purposes) of the use or conduct of the source is to obtain legally privileged information.

3.7 This assessment will be taken into account by the authorizing officer in deciding whether the proposed use or conduct of a source is necessary and proportionate for a purpose under Article 35 of the Law. The authorizing officer may require regular reporting so as to be able to decide whether the authorization should continue. In those cases where legally privileged information has been acquired and retained, the matter should be reported to the Commissioner or Inspector during his or her next inspection and the material should be made available to him or her if requested.

3.8 A substantial proportion of the communications between a lawyer and his client(s) may be subject to legal privilege. Therefore, any case where a lawyer is the subject of an investigation or operation should be notified to the Commissioner or Inspector during his or her next inspection and any material which has been retained should be made available to him or her if requested.

3.9 Where there is any doubt as to the handling and dissemination of information which may be subject to legal privilege, advice should be sought from the Law Officers' Department before any further dissemination of the material takes place. Similar advice should also be sought where there is doubt over whether information is not subject to legal privilege due to the "in furtherance of a criminal purpose" exception. The retention of legally privileged information, or its dissemination to an outside body, should be accompanied by a clear warning that it is subject to legal privilege. It should be safeguarded by taking reasonable steps to ensure there is no possibility of it becoming available, or its contents becoming known to any person whose possession of it might prejudice any criminal or civil proceedings related to the information. Any dissemination of legally privileged material to an outside body should be notified to the relevant Commissioner or Inspector during his next inspection.

Communications involving Confidential Personal Information and Confidential Journalistic Material

3.10 Similar consideration must also be given to authorizations that involve confidential personal information and confidential journalistic material. In those cases where confidential personal information and confidential journalistic material has been acquired and retained, the matter should be reported to the Commissioner or Inspector during his or her next inspection and the material be made available to him or her if requested. Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling concerning an individual (whether living or dead) who can be identified from it. Such information, which can include both oral and written communications is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. Examples might include consultations between a health professional and a patient, or information from a patient's medical records.

3.11 Spiritual counselling means conversations between an individual and a Minister of Religion acting in his or her official capacity, where the

individual being counselled is seeking or the Minister is imparting forgiveness, absolution or the resolution of conscience with the authority of the Divine Being(s) of their faith.

3.12 Confidential journalistic material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.

Vulnerable individuals

3.13 A 'vulnerable individual' is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself or herself, or unable to protect himself or herself against significant harm or exploitation. Any individual of this description should only be authorized to act as a source in the most exceptional circumstances and only after advice has been sought from the Law Officers' Department.

Juvenile sources

3.14 Special safeguards also apply to the use or conduct of juvenile sources; that is sources under the age of 18 years. **On no occasion should the use or conduct of a source under 16 years of age be authorized to give information against his or her parents or any person who has parental responsibility for the source**. In other cases, authorizations should not be granted unless special provisions prescribed by the Minister are satisfied. It is recommended that the grant of authority to use a source under 16 years of Attorney General is considered at a senior level in the public authority. The duration of such an authorization is one month instead of 12 months.

4 AUTHORIZATION PROCEDURES FOR COVERT HUMAN INTELLIGENCE SOURCES

4.1 Under Article 32(7) of the Law a person is a source if:

(a) he or she establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c);

(b) he or she covertly uses such a relationship to obtain information or to provide access to any information to another person; or

(c) he or she covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

4.2 A source may include those referred to as agents, informants and officers working undercover.

4.3 By virtue of Article 32(9)(b) of the Law a purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if and only if, the relationship is conducted in a manner that is calculated to

ensure that one of the parties to the relationship is unaware of the purpose.

4.4 By virtue of Article 32(9)(c) of the Law a relationship is used covertly, and information obtained as mentioned in paragraph 4.1(c) above is disclosed covertly, if and only if it is used or, as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

4.5 The use of a source involves inducing, asking or assisting a person to engage in the conduct of a source or to obtain information by means of the conduct of such a source.

4.6 The conduct of a source is any conduct falling within Article 35(4) of the Law, or which is incidental to anything falling within Article 35(4) of the Law.

Authorization procedures

4.7 Under Article 35(3) of the Law an authorization for the use or conduct of a source may be granted by the authorizing officer where he believes that the authorization is necessary:

- in the interests of national security[12][13];
- for the purpose of preventing and detecting[14] crime or of preventing disorder;
- in the interests of the economic well-being of Jersey;
- in the interests of public safety;
- for the purpose of protecting public health[15]
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or
- for any other purpose prescribed in an Order made by the Minister for Home Affairs.[16]

4.8 The authorizing officer must also believe that the authorized use or conduct of a source is proportionate to what is sought to be achieved by that use or conduct.

[12] One of the functions of the Security Service is the protection of national security and, in particular, the protection of threats from internal terrorism and some of these functions may extend to Jersey. An authorizing officer in another public authority should not issue an authorization under Part 3 of the Law where the operation or investigation falls within the responsibility of he Security Service, except where it is a directed surveillance investigation or operation and the Security Service has agreed that another authority should carry out.

[13] HM Forces may also undertake operations in connection with a military threat to national security and other operations in connection with national security in support of the Security Service.

[14] Detecting crime is defined in Article 1(2) of the Law.

[15] This could include investigations into infectious diseases, contaminated products or the illicit sale of pharmaceuticals.

[16] This could only be for a purpose which satisfies the criteria set out in Article 8(2) of the ECHR.

4.9 The public authorities entitled to authorize the use or conduct of a source are those listed in Schedule 1 to the Law. Responsibility for authorizing the use or conduct of a source rests with the authorizing officer and all authorizations require the personal authority of the authorizing officer. An authorizing officer is the person designated under Article 36 of the Law to grant an authorization for the use or conduct of a source. In certain circumstances the Attorney General will be the authorizing officer (see Article 36 of the Law).

4.10 The authorizing officer must give authorizations in writing, except that in urgent cases, they may be given orally by the authorizing officer. In such cases, a statement that the authorizing officer has expressly authorized the action should be recorded in writing by the applicant as soon as is reasonably practicable.

4.11 A case is not normally to be regarded as urgent unless the time that would elapse before the authorizing officer was available to grant the authorization would, in the judgement of the person giving the authorization, be likely to endanger life or jeopardise the operation or investigation for which the authorization was being given. An authorization is not to be regarded as urgent where the need for an authorization has been neglected or the urgency is of the authorizing officer's own making.

4.12 The Chief Officer, Agent of the Impôts or Chief Inspector of Immigration may only grant authorizations on application by a member of their own force or Service.

Information to be provided in applications for authorization

4.13 An application for authorization for the use or conduct of a source should be in writing and record:

- the reasons why the authorization is necessary in the particular case and on the grounds (e.g. for the purpose of preventing or detecting crime) listed in Article 35(3) of the Law;
- the reasons why the authorization is considered proportionate to what it seeks to achieve;
- the purpose for which the source will be tasked or deployed (e.g. in relation to an organised serious crime, espionage, a series of racially motivated crimes etc);
- where a specific investigation or operation is involved, nature of that investigation or operation;
- the nature of what the source will be tasked to do;
- the level of authority required (or recommended, where that is different);
- the details of any potential collateral intrusion and why the intrusion is justified;
- the details of any confidential information that is likely to be obtained as a consequence of the authorization; and

- a subsequent record of whether authority was given or refused, by whom and the time and date.

4.14 Additionally, in urgent cases, the authorization should record the reasons why the authorizing officer considered the case so urgent that an oral instead of a written authorization was given.

4.15 Where the authorization is oral, the detail referred to above should be recorded in writing by the applicant as soon as reasonably practicable.

Duration of authorizations

4.16 A written authorization will, unless renewed, cease to have effect at the end of a period of **12 months** beginning with the day on which it took effect.

4.17 Urgent oral authorizations will, unless renewed, cease to have effect after **72 hours**, beginning with the time when the authorization was granted or renewed.

Reviews

4.18 Regular reviews of authorizations should be undertaken to assess the need for the use of a source to continue. The review should include the use made of the source during the period authorized, the tasks given to the source and the information obtained from the source. The results of a review should be recorded on the authorization record (see paragraphs 2.13 - 2.15). Particular attention is drawn to the need to review authorizations frequently where the use of a source provides access to confidential information or involves collateral intrusion.

4.19 In each case the authorizing officer within each public authority should determine how often a review should take place. This should be as frequently as is considered necessary and practicable.

Renewals

4.20 Before an authorizing officer renews an authorization, he or she must be satisfied that a review has been carried out of the use of a source as outlined in paragraph 4.19.

4.21 If at any time before an authorization would cease to have effect, the authorizing officer considers it necessary for the authorization to continue for the purpose for which it was given, the officer may renew it in writing for a further period of **12 months**. Renewals may also be granted orally in urgent cases and last for a period of **72 hours**.

4.22 A renewal takes effect at the time at which, or day on which the authorization would have ceased to have effect but for the renewal. An application for renewal should not be made until shortly before the authorization period is drawing to an end. Any person who would be entitled to grant a new authorization can renew an authorization. Authorizations may be renewed more than once, if necessary, provided they continue to meet the criteria for authorization. The renewal should be kept/recorded as part of the authorization record (see paragraphs 2.13 - 2.15).

4.23 All applications for the renewal of an authorization should record:

- whether this is the first renewal or every occasion on which the authorization has been renewed previously;
- any significant changes to the information in paragraph 4.14;
- the reasons why it is necessary to continue to use the source;
- the use made of the source in the period since the grant or, as the case may be, latest renewal of the authorization;
- the tasks given to the source during that period and the information obtained from the conduct or use of the source;
- the results of regular reviews of the use of the source.

Cancellations

4.24 The authorizing officer who granted or renewed the authorization must (or his or her deputy) cancel it if the officer is satisfied that the use or conduct of the source no longer satisfies the criteria for authorization or that satisfactory arrangements for the source's case no longer exist. Where the authorizing officer is no longer available, this duty will fall on the person who has taken over the rôle of authorizing officer or the person who is acting as authorizing officer in accordance with an Order of the Minister for Home Affairs under Article 41(4) of the Law. Where necessary, the safety and welfare of the source should continue to be taken into account after the authorization has been cancelled.

Management of Sources

Tasking

4.25 Tasking is the assignment given to the source by the persons defined at Articles 35(5)(a) and (b) of the Law, asking the source to obtain information, to provide access to information or to otherwise act, incidentally, for the benefit of the relevant public authority. Authorization for the use or conduct of a source is required prior to any tasking where such tasking requires the source to establish or maintain a personal or other relationship for a covert purpose.

4.26 The person referred to in Article 35(5)(a) of the Law will have day to day responsibility for:

- dealing with the source on behalf of the authority concerned;
- directing the day to day activities of the source;
- recording the information supplied by the source; and
- monitoring the source's security and welfare.

4.27 The person referred to in Article 35(5)(b) of the Law will be responsible for the general oversight of the use of the source.

4.28 In some instances, the tasking given to a person will not require the source to establish a personal or other relationship for a covert purpose. For example a source may be tasked with finding out purely factual information about the layout of commercial premises. Alternatively, a trading standards officer may be involved in the test purchase of items which have been labelled misleadingly or are unfit for consumption. In

such cases, it is for the relevant public authority to determine where, and in what circumstances, such activity may require authorization.

4.29 It is not the intention that authorizations be drawn so narrowly that a separate authorization is required each time the source is tasked. Rather, an authorization might cover, in broad terms, the nature of the source's task. If this changes, then a new authorization may need to be sought.

4.30 It is difficult to predict exactly what might occur each time a meeting with a source takes place, or the source meets the subject of an investigation. There may be occasions when unforeseen action or undertakings occur. When this happens, the occurrence must be recorded as soon as practicable after the event and, if the existing authorization is insufficient it should either be updated and reauthorized (for minor amendments only) or it should cancelled and a new authorization should be obtained before any further such action is carried out.

4.31 Similarly where it is intended to task a source in a new way or significantly greater way than previously identified, the persons defined at Article 35(5)(a) or (b) of the Law must refer the proposed tasking to the authorizing officer, who should consider whether a separate authorization is required. This should be done in advance of any tasking and the details of such referrals must be recorded.

Management responsibility

4.32 Public authorities should ensure that arrangements are in place for the proper oversight and management of sources, including appointing individual officers as defined in Article 35(5)(a) and (b) of the Law for each source.

4.33 The person responsible for the day-to-day contact between the public authority and the source will usually be of a rank or position below that of the authorizing officer.

4.34 In cases where the authorization is for the use or conduct of a source whose activities benefit more than a single public authority, responsibilities for the management and oversight of that source may be taken up by one authority or can be split between the authorities.

Security and welfare

4.35 Any public authority deploying a source should take into account the safety and welfare of that source, when carrying out actions in relation to an authorization or tasking, and to foreseeable consequences to others of that tasking. Before authorizing the use or conduct of a source, the authorizing officer should ensure that a risk assessment is carried out to determine the risk to the source of any tasking and the likely consequences should the role of the source become known. The ongoing security and welfare of the source, after the cancellation of the authorization, should also be considered at the outset.

4.36 The person defined at Article 35(5)(a) of the Law is responsible for bringing to the attention of the person defined at Article 35(5)(b) of the Law any concerns about the personal circumstances of the source, insofar as they might affect:

- the validity of the risk assessment

- the conduct of the source, and
- the safety and welfare of the source.

4.37 Where deemed appropriate, concerns about such matters must be considered by the authorizing officer, and a decision taken on whether or not to allow the authorization to continue.

Additional Rules

Recording of telephone conversations

4.38 Subject to paragraph 4.40, the interception of communications sent by post or by means of public telecommunications systems or private telecommunications systems attached to the public network may be authorized only by the Attorney General, in accordance with the terms of Part 2 of the Law. Nothing in this code should be taken as granting dispensation from the requirements of that Part of the Law.

4.39 Part 2 of the Law provides certain exceptions to the rule that interception of telephone conversations must be warranted under that Part. This includes, where one party to the communication consents to the interception, it may be authorized in accordance with Articles 30(4) and 31(4) of the Law provided that there is no interception warrant authorizing the interception. In such cases, the interception is treated as directed surveillance (see chapter 4 of the Covert Surveillance code of practice).

Use of covert human intelligence source with technical equipment

4.40 A source, whether or not wearing or carrying a surveillance device and invited into residential premises or a private vehicle, does not require additional authorization to record any activity taking place inside those premises or vehicle which take place in his presence. This also applies to the recording of telephone conversations other than by interception which takes place in the source's presence. Authorization for the use or conduct of that source may be obtained in the usual way.

4.41 However, if a surveillance device is to be used, other than in the presence of the source, an intrusive surveillance authorization and if applicable an authorization for interference with property should be obtained.

5 OVERSIGHT BY COMMISSIONERS

5.1 The Law requires the Commissioner to keep under review (with the assistance of the Assistant Surveillance Commissioners) the performance of functions under Part 11 of PPCE and Part 3 of the Law by the police and of the Law the other public authorities listed in Schedule 1.

5.2 This code does not cover the exercise of any of the Commissioner's functions. It is the duty of any person who uses these powers to comply with any request made by the Commissioner to disclose or provide any information the Commissioner requires for the purpose of enabling the Commissioner to carry out his or her functions.

5.3 References in this code to the performance of review functions by the Commissioner apply also to Inspectors and other members of staff to whom such functions have been delegated.

6 COMPLAINTS

6.1 The Law establishes an independent Tribunal. This Tribunal will be made up of senior members of the judiciary and the legal profession and is independent of States. The Tribunal has full powers to investigate and decide any case within its jurisdiction.

6.2 This code does not cover the exercise of the Tribunal's functions. Details of the relevant complaints procedure can be obtained from the following address:

The Secretary
Investigatory Powers Tribunal
States Greffe
Jersey
JE1 1DD

[1] *L.17/2005*