

# THIRD SUPPLEMENT TO THE GIBRALTAR GAZETTE

No. 5311 GIBRALTAR Wednesday 10th June 2026

---

B. 23/26

## INVESTIGATORY POWERS BILL 2026

### ARRANGEMENT OF CLAUSES

1. Title and commencement.
2. General definitions.
3. Telecommunications definitions.
4. Postal definitions.
5. General definitions: journalistic material etc.

### PART 1

#### GENERAL PRIVACY PROTECTIONS

6. Overview of Act.
7. General duties in relation to privacy.
8. Offence of unlawful interception.
9. Definition of “interception” etc.
10. Conduct that is not interception.
11. Definition of lawful authority.
12. Monetary penalties for certain unlawful interceptions.
13. Civil liability for certain unlawful interceptions.
14. Restriction on requesting interception by overseas authorities.
15. Restriction on requesting assistance under mutual assistance agreements.
16. Offence of unlawfully obtaining communications data.
17. Mandatory use of equipment interference authorisations.

### PART 2

#### LAWFUL INTERCEPTION OF COMMUNICATIONS

18. Authorisations that may be granted under this Chapter.
19. Obtaining secondary data.
20. Subject-matter of authorisations.
21. Persons who may apply for the grant of an authorisation.
22. Power of the competent authority to grant authorisations.
23. Grounds on which authorisations may be granted.

24. Members of Parliament etc.
25. Items subject to legal privilege.
26. Confidential journalistic material.
27. Sources of journalistic information.
28. Grant of authorisations.
29. Requirements that must be met by authorisations.
30. Duration of authorisations.
31. Renewal of authorisations.
32. Modification of authorisations.
33. Further provision about modifications.
34. Cancellation of authorisations.
35. Special rules for certain mutual assistance authorisations.
36. Implementation of authorisations.
37. Service of authorisations.
38. Duty of operators to assist with implementation.
39. Interception with the consent of the sender or recipient.
40. Interception by providers of postal or telecommunications services.
41. Interception for monitoring and record-keeping purposes.
42. Postal services: Interception for enforcement purposes.
43. Interception by the Gibraltar Regulatory Authority (“GRA”) in connection with radiocommunication.
44. Interception in prisons.
45. Interception in accordance with overseas requests.
46. Safeguards relating to retention and disclosure of material.
47. Safeguards relating to disclosure of material overseas.
48. Additional safeguards for items subject to legal privilege.
49. Exclusion of matters from legal proceedings etc.
50. Duty not to make unauthorised disclosures.
51. Section 50: meaning of “excepted disclosure”.
52. Offence of making unauthorised disclosures.
53. Part 2: interpretation.

### **PART 3**

#### **AUTHORISATIONS FOR OBTAINING COMMUNICATIONS DATA**

54. Power to grant authorisations.
55. Restrictions in relation to internet connection records.
56. Procedure for authorisations under this Part.
57. Duration and cancellation of authorisations.
58. Duties of telecommunication operators in relation to authorisations.
59. Further provisions on grant of authorisations.
60. Lawfulness of conduct authorised by an authorisation granted under this Part.
61. Offence of making unauthorised disclosure.
62. Application of Part 3 to postal operators and postal services.
63. Extra-territorial application of Part 3.
64. Part 3: interpretation.

## **PART 4**

### **EQUIPMENT INTERFERENCE**

65. Authorisations under this Part: general.
66. Meaning of “equipment data”.
67. Subject-matter of authorisations.
68. Power to grant equipment interference authorisations.
69. Restriction on grant of targeted equipment interference authorisations.
70. Members of Parliament, etc.
71. Items subject to legal privilege.
72. Confidential journalistic material.
73. Sources of journalistic information.
74. Requirements that must be met by targeted equipment interference authorisations.
75. Duration of targeted equipment interference authorisations.
76. Renewal of targeted equipment interference authorisations.
77. Modification of targeted equipment interference authorisations.
78. Cancellation of targeted equipment interference authorisations.
79. Implementation of targeted equipment interference authorisations.
80. Service of authorisations.
81. Duty of telecommunications operators to assist with implementation.
82. Safeguards relating to retention and disclosure of material.
83. Safeguards relating to disclosure of material overseas.
84. Additional safeguards for items subject to legal privilege.
85. Duty not to make unauthorised disclosures.
86. Section 85: meaning of “excepted disclosure”.
87. Offence of making unauthorised disclosure.
88. Part 4: interpretation.

## **PART 5**

### **SURVEILLANCE AND COVERT INVESTIGATIONS AND ENTRY ON OR INTERFERENCE WITH PROPERTY AND RADIOCOMMUNICATION**

89. Conduct to which Chapter 1 applies.
90. Lawful surveillance, etc.
91. Authorisations for directed surveillance.
92. Authorisations for intrusive surveillance.
93. Authorisations for covert human intelligence sources.
94. Covert human intelligence sources: criminal conduct authorisations.
95. Criminal conduct authorisations: safeguards for juveniles.
96. Criminal conduct authorisations: safeguards for vulnerable adults.
97. Procedure for authorisations: directed surveillance, standard covert human intelligence sources and standard criminal conduct authorisations.
98. Procedure for authorisations: intrusive surveillance, covert human intelligence sources involving a juvenile source or a vulnerable adult and criminal conduct authorisations involving a juvenile source or a vulnerable adult.
99. General rules about grant, renewal and duration.

100. Cancellation of authorisations by the competent authority.
101. Cancellation of authorisations by an intercepting authority.
102. Entry on or interference with property or radio communication.
103. Authorisations to enter on or interfere with property or radio communication.
104. Authorisations: form and duration.
105. Power to extend or modify authorisations.
106. Matters subject to legal privilege: covert human intelligence sources.
107. Interpretation of Part 5.

## **PART 6**

### **INVESTIGATION OF ELECTRONIC DATA PROTECTED BY ENCRYPTION, ETC.**

108. Notices requiring disclosure (“Disclosure notices”).
109. Effect of notice imposing disclosure requirement.
110. Cases in which key required.
111. Arrangements for payments of disclosure.
112. Failure to comply with a notice.
113. Tipping-off.
114. General duties of specified authorities.
115. Interpretation of Part 6.

## **PART 7**

### **OVERSIGHT ARRANGEMENTS**

116. Investigatory Powers Commissioner.
117. Terms and conditions of appointment.
118. Main oversight functions.
119. Additional directed oversight functions.
120. Error reporting.
121. Additional functions under this Part.
122. Functions under other Parts and other enactments.
123. Annual and other reports.
124. Investigatory and information powers.
125. Information gateway.
126. Power to modify functions.
127. Codes of practice.
128. Appeals to the Court of Appeal.

## **PART 8**

### **MISCELLANEOUS AND GENERAL PROVISIONS**

129. Urgent authorisation granted by an intercepting authority.
130. Notification of urgent authorisations to competent authority.

- 131. The competent authority.
- 132. Terms and conditions of appointment.
- 133. Combination of authorisations and notices.
- 134. Payments towards certain compliance costs.
- 135. Power to develop compliance systems etc.
- 136. Foreign surveillance operations (“continued surveillance”).
- 137. Offences by bodies corporate etc.
- 138. Territorial application of this Act.
- 139. Regulations and Orders.
- 140. Financial provisions.
- 141. Transitional, transitory or saving provision.
- 142. Minor and consequential provision.

### **SCHEDULE 1**

#### **Monetary Penalty Notices**

### **SCHEDULE 2**

#### **Exceptions to Section 49**

### **SCHEDULE 3**

#### **Combination of Authorisations and Notices**

### **SCHEDULE 4**

#### **Targeted Interception Authorisation Members of Parliament, etc. – Additional Safeguards**

### **SCHEDULE 5**

#### **Targeted Equipment Interference Authorisation Members of Parliament, etc. – Additional Safeguards**

### **SCHEDULE 6**

#### **Conditions on “Continued Surveillance”**



# THIRD SUPPLEMENT TO THE GIBRALTAR GAZETTE

No. 5311 GIBRALTAR Wednesday 10th June 2026

---

B. 23/26

## BILL

### FOR

**AN ACT** to make provision for and about the interception of communications, the acquisition of communications data and equipment interference; to make provision about the treatment of material held as a result of such interception, acquisition or equipment interference; to make provision for the carrying out of surveillance and entry on or interference with property and radiocommunication, the use of covert human intelligence sources and the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed; to provide for the Investigatory Powers Commissioner and the competent authority and make provision about them and other oversight arrangements; to make further provision about investigatory powers, intercepting authorities and the security of Gibraltar and for connected purposes.

**ENACTED** by the Legislature of Gibraltar.

#### **Title and commencement.**

1.(1) This Act may be cited as the Investigatory Powers Act 2026.

(2) This Act comes into operation on the day appointed by the Government by notice in the Gazette.

(3) Different dates may be appointed under subsection (2) for different provisions.

#### **General**

##### *Interpretation*

#### **General definitions.**

2.(1) In this Act-

"apparatus" includes any equipment, machinery or device (whether physical or logical) and any wire or cable;

"civil proceedings" means any proceedings in or before any court that are not criminal proceedings;

“Collector of Customs” means the Collector appointed under section 3 of the Imports and Exports Act, 1986;

“Commissioner of Police” means the person appointed to be Commissioner of Police under the Police Act 2006;

“competent authority” means such person appointed by the Chief Minister pursuant to section 131;

"crime" means conduct which-

- (a) constitutes one or more criminal offences; or
- (b) is, or corresponds to, any conduct which, if it all took place in Gibraltar, would constitute one or more criminal offences;

"criminal proceedings" has the same meaning as in the Criminal Procedure and Evidence Act 2011 (see section 2 of that Act);

“customs officer” means an officer appointed under section 3 of the Imports and Exports Act, 1986;

"data" includes data which is not electronic data and any information (whether or not electronic);

"destroy", in relation to electronic data, means delete the data in such a way as to make access to the data impossible (and related expressions are to be read accordingly);

"enactment" means an enactment whenever passed or made; and includes an enactment passed after this Act and includes subsidiary legislation;

"functions" includes powers and duties;

“guardian” in relation to a juvenile source, means a guardian appointed in accordance with section 15 of the Children Act 2009;

"high judicial office" means judicial office as a judge of a court having unlimited jurisdiction in civil and criminal matters in some part of the Commonwealth or in Ireland, or of a court having jurisdiction in appeals from any such court;

“HM Customs Gibraltar” means a law enforcement body and import authority under the Imports and Exports Act, 1986;

"identifying data" has the meaning given by subsection (2);

"intercepting authority" means-

- (a) the Commissioner of Police or in his absence an appropriate delegate appointed by him acting as Commissioner of Police;
- (b) the Collector of Customs or in his absence an appropriate delegate appointed by him acting as Collector of Customs;
- (c) such other person as may be designated by an order made by the Minister (such order may impose restrictions on the circumstances in which, or the purposes for which, such authorisation or notice may be applied for or granted).

"the Investigatory Powers Commissioner" means the person appointed under section 116(1);

"items subject to legal privilege" has the same meaning as in the Criminal Procedure and Evidence Act 2011(see section 2 of that Act);

"legal proceedings" means civil or criminal proceedings in or before a court;

"Minister" means the Minister with responsibility for Justice or such other person as the Chief Minister may nominate;

"modify" includes amend, repeal or revoke (and related expressions are to be read accordingly);

"person holding office under the Crown in right of the Government of Gibraltar" includes any servant of the Crown in right of the Government of Gibraltar;

"police officer" has the definition given to it under section 2 of the Police Act 2006;

"premises" includes any land, movable structure, vehicle, vessel, aircraft or hovercraft (and "set of premises" is to be read accordingly);

"public authority" includes the competent authority, an intercepting authority, a telecommunications operator, a postal operator and any person whose functions are functions of a public nature, but does include a court or tribunal, Parliament or a person exercising functions in connection with proceedings in Parliament.

"radiocommunication" and "radiocommunication apparatus" have the same meaning as in the Communications Act 2006;

"relative" has the meaning given in section 2 of the Children Act 2009;

"relevant confidential information" means information which is held in confidence by a member of a profession and consists of-

(a) personal records or journalistic material which are (or would be if held in Gibraltar) excluded material as defined by section 15 of the Criminal Procedure and Evidence Act 2011; or

(b) communications between Members of Parliament and their constituents,

and the references in this paragraph to a member of a profession include references to any person acting in the course of any trade, business, profession or other occupation or for the purposes of any paid or unpaid office.

“Royal Gibraltar Police” means the force established under the Police Act 2006 designated the Royal Gibraltar Police;

"serious crime" means crime where-

(a) the offence, or one of the offences, which is or would be constituted by the conduct concerned is an offence for which a person who has reached the age of 18 and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of 3 years or more; or

(b) the conduct involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose;

"source of journalistic information" means an individual who provides material intending the recipient to use it for the purposes of journalism or knowing that it is likely to be so used;

"specified", in relation to an authorisation, notice or regulations, means specified or described in the authorisation, notice or (as the case may be) regulations (and "specify" is to be read accordingly);

“standard covert human intelligence source” means a covert human intelligence source which does not involve a juvenile source or a vulnerable adult source;

“standard criminal conduct authorisation” means a criminal conduct authorisation which does not involve a juvenile source or a vulnerable adult source;

"statutory", in relation to any function, means conferred by virtue of this Act or any other enactment or subsidiary legislation;

"systems data" has the meaning given by subsection (4);

"working day" means a day other than a Saturday, a Sunday, Christmas Day, Good Friday or a bank holiday under the Banking and Financial Dealings Act .

(2) In this Act "identifying data" means data which may be used to identify, or assist in identifying -

- (a) any person, apparatus, system or service;
- (b) any event; or
- (c) the location of any person, event or thing.

(3) For the purposes of subsection (2), the reference to data which may be used to identify, or assist in identifying, any event includes data relating to the-

- (a) fact of the event;
- (b) type, method or pattern of event;
- (c) time or duration of the event.

(4) In this Act "systems data" means any data that enables or facilitates, or identifies or describes anything connected with enabling or facilitating, the functioning of any of the following-

- (a) a postal service;
- (b) a telecommunication system (including any apparatus forming part of the system);
- (c) any telecommunications service provided by means of a telecommunication system;
- (d) a relevant system (including any apparatus forming part of the system);
- (e) any service provided by means of a relevant system.

(5) For the purposes of subsection (4), a system is a "relevant system" if any communications or other information are held on or by means of the system.

(6) For the purposes of this Act detecting crime or serious crime is to be taken to include-

- (a) establishing by whom, for what purpose, by what means and generally in what circumstances any crime or (as the case may be) serious crime was committed; and
- (b) the apprehension of the person by whom any crime or (as the case may be) serious crime was committed.

(7) References in this Act to the examination of material obtained under an authorisation are references to the material being read, looked at or listened to by the persons to whom it becomes available as a result of the authorisation.

**Telecommunications definitions.**

3.(1) The definitions in this section have effect for the purposes of this Act.

*Communication*

(2) "Communication", in relation to a telecommunications operator, telecommunications service or telecommunication system, includes-

- (a) anything comprising speech, music, sounds, visual images or data of any description; and
- (b) signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus.

*Entity data*

(3) "Entity data" means any data which-

- (a) is about-
  - (i) an entity;
  - (ii) an association between a telecommunications service and an entity; or
  - (iii) an association between any part of a telecommunication system and an entity; and
- (b) consists of, or includes, data which identifies or describes the entity (whether or not by reference to the entity's location); and
- (c) is not events data.

*Events data*

(4) "Events data" means any data which identifies or describes an event (whether or not by reference to its location) on, in or by means of a communication system where the event consists of one or more entities engaging in a specific activity at a specific time.

*Communications data*

(5) "Communications data", in relation to a telecommunications operator, telecommunications service or telecommunication system, means entity data or events data-

- (a) which is (or is to be or is capable of being) held or obtained by, or on behalf of, a telecommunications operator and-
  - (i) is about an entity to which a telecommunications service is provided and relates to the provision of the service;
  - (ii) is comprised in, included as part of, attached to or logically associated with a communication (whether by the sender or otherwise) for the purposes of a telecommunication system by means of which the communication is being or may be transmitted; or
  - (iii) does not fall within sub-paragraph (i) or (ii) but does relate to the use of a telecommunications service or a telecommunication system;
- (b) which is available directly from a telecommunication system and falls within sub-paragraph (ii) of paragraph (a); or
- (c) which-
  - (i) is (or is to be or is capable of being) held or obtained by, or on behalf of, a telecommunications operator;
  - (ii) is about the architecture of a telecommunication system; and
  - (iii) is not about a specific person,

but does not include any content of a communication or anything which, in the absence of subsection (6)(b), would be content of a communication.

#### *Content of a communication*

(6) "Content", in relation to a communication and a telecommunications operator, telecommunications service or telecommunication system, means any element of the communication, or any data attached to or logically associated with the communication, which reveals anything of what might reasonably be considered to be the meaning (if any) of the communication, but-

- (a) any meaning arising from the fact of the communication or from any data relating to the transmission of the communication is to be disregarded; and
- (b) anything which is systems data is not content.

#### *Other definitions*

(7) "Entity" means a person or thing.

(8) "Public telecommunications service" means any telecommunications service which is offered or provided to the public, or a substantial section of the public, in any one or more parts of Gibraltar.

(9) "Public telecommunication system" means a telecommunication system located in Gibraltar-

- (a) by means of which any public telecommunications service is provided; or
- (b) which consists of parts of any other telecommunication system by means of which any such service is provided.

(10) "Telecommunications operator" means a person who-

- (a) offers or provides a telecommunications service to persons in Gibraltar; or
- (b) controls or provides a telecommunication system which is (wholly or partly)-
  - (i) in Gibraltar; or
  - (ii) controlled from Gibraltar.

(11) "Telecommunications service" means any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the person providing the service).

(12) For the purposes of subsection (11), the cases in which a service is to be taken to consist in the provision of access to, and of facilities for making use of, a telecommunication system include any case where a service consists in or includes facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of such a system.

(13) "Telecommunication system" means a system (including the apparatus comprised in it) that exists (whether wholly or partly in Gibraltar or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electromagnetic energy.

(14) "Private telecommunication system" means any telecommunication system which-

- (a) is not a public telecommunication system;
- (b) is attached, directly or indirectly, to a public telecommunication system (whether or not for the purposes of the communication in question); and
- (c) includes apparatus which is both located in Gibraltar and used (with or without other apparatus) for making the attachment to that public telecommunication system.

**Postal definitions.**

4.(1) The definitions in this section have effect for the purposes of this Act.

*Communication*

(2) "Communication", in relation to a postal operator or postal service (but not in the definition of "postal service" in this section), includes anything transmitted by a postal service.

*Communications data*

(3) "Communications data", in relation to a postal operator or postal service, means-

- (a) postal data comprised in, included as part of, attached to or logically associated with a communication (whether by the sender or otherwise) for the purposes of a postal service by means of which it is being or may be transmitted;
- (b) information about the use made by any person of a postal service (but excluding any content of a communication (apart from information within paragraph (a))); or
- (c) information not within paragraph (a) or (b) that is (or is to be or is capable of being) held or obtained by or on behalf of a person providing a postal service, is about those to whom the service is provided by that person and relates to the service so provided.

*Postal data*

(4) "Postal data" means data which-

- (a) identifies, or purports to identify, any person, apparatus or location to or from which a communication is or may be transmitted;
- (b) identifies or selects, or purports to identify or select, apparatus through which, or by means of which, a communication is or may be transmitted;
- (c) identifies, or purports to identify, the time at which an event relating to a communication occurs; or
- (d) identifies the data or other data as data comprised in, included as part of, attached to or logically associated with a particular communication.

For the purposes of this definition "data", in relation to a postal item, includes anything written on the outside of the item.

*Other definitions*

- (5) "Postal item" means-
- (a) any letter, postcard or other such thing in writing as may be used by the sender for imparting information to the recipient; or
  - (b) any packet or parcel.
- (6) "Postal operator" means a person providing a postal service to persons in Gibraltar.
- (7) "Postal service" means services involving the collection, clearance, sorting, transport and distribution of postal items as per the Post Office Act;
- (8) "Public postal service" means a postal service that is offered or provided to the public, or a substantial section of the public in Gibraltar.

**General definitions: "journalistic material" etc.**

5.(1) The definitions in this section have effect for the purposes of this Act.

*Journalistic material*

- (2) "Journalistic material" means material created or acquired for the purposes of journalism.
- (3) For the purposes of this section, where-
- (a) a person ("R") receives material from another person ("S"); and
  - (b) S intends R to use the material for the purposes of journalism,

R is to be taken to have acquired it for those purposes.

Accordingly, a communication sent by S to R containing such material is to be regarded as a communication containing journalistic material.

(4) For the purposes of determining whether a communication contains material acquired for the purposes of journalism, it does not matter whether the material has been acquired for those purposes by the sender or recipient of the communication or by some other person.

- (5) For the purposes of this section-
- (a) material is not to be regarded as created or acquired for the purposes of journalism if it is created or acquired with the intention of furthering a criminal purpose; and
  - (b) material which a person intends to be used to further such a purpose is not to be regarded as intended to be used for the purposes of journalism.

*Confidential journalistic material*

- (6) "Confidential journalistic material" means-
- (a) in the case of material contained in a communication, journalistic material which the sender of the communication-
    - (i) holds in confidence; or
    - (ii) intends the recipient, or intended recipient, of the communication to hold in confidence;
  - (b) in any other case, journalistic material which a person holds in confidence.
- (7) A person holds material in confidence for the purposes of this section if-
- (a) the person holds it subject to an express or implied undertaking to hold it in confidence; or
  - (b) the person holds it subject to a restriction on disclosure or an obligation of secrecy contained in an enactment.

**PART 1**

**General Privacy Protections**

*Overview and General Privacy Duties*

**Overview of Act**

6.(1) This Act sets out the extent to which certain investigatory powers may be used to interfere with privacy.

(2) This Part imposes certain duties in relation to privacy and contains other protections for privacy.

- (3) These other protections include offences and penalties in relation to the unlawful-
- (a) interception of communications, and
  - (b) obtaining of communications data.

(4) Further protections for privacy-

- (a) can be found, in particular, in the regimes provided for by Parts 2 to 4 and in the oversight arrangements in Part 7; and
- (b) also exist-
  - (i) by virtue of the Gibraltar Constitution Order 2006;
  - (ii) in section 175 of the Data Protection Act 2004 (unlawful obtaining etc. of personal data);
  - (iii) in section 76(2) of the Communications Act 2006 (misleading messages and interception and disclosure of messages);
  - (iv) in sections 362 to 366A of the Crimes Act 2011 (computer misuse offences);
  - (v) in the common law offence of misconduct in public office; and
  - (vi) elsewhere in the law.

(5) The regimes provided for by Parts 2 to 4 are as follows-

- (a) Part 2 sets out circumstances (including under an authorisation) in which the interception of communications is lawful and make further provision about the interception of communications and the treatment of material obtained in connection with it;
- (b) Part 3 sets out circumstances in which the obtaining of communications data is lawful in pursuance of an authorisation and make further provision about the obtaining and treatment of such data; and
- (c) Part 4 deals with equipment interference authorisations.

(6) As to the rest of the Act-

- (a) Part 5 deals with surveillance, covert investigations and entry on or interference with property and radiocommunication;
- (b) Part 6 makes provision for the investigation of electronic data protected by encryption;
- (c) Part 7 deals with oversight arrangements for regimes in this Act and elsewhere; and

(d) Part 8 contains miscellaneous and general provisions including combined authorisations and notices.

(7) The Minister may by order amend the Schedules in this Act.

**General duties in relation to privacy.**

7.(1) Subsection (2) applies where the competent authority is deciding whether-

- (a) to grant, renew, cancel or modify an authorisation under Parts 2, 3, 4 or 5; or
- (b) to grant, vary or revoke a notice under Part 6.

(2) The competent authority must have regard to-

- (a) whether what is sought to be achieved by the authorisation or notice could reasonably be achieved by other less intrusive means;
- (b) whether the level of protection to be applied in relation to any obtaining of information by virtue of the authorisation or notice is higher because of the particular sensitivity of that information;
- (c) the public interest in the integrity and security of telecommunication systems and postal services; and
- (d) any other aspects of the public interest in the protection of privacy.

(3) The duties under subsection (2)-

- (a) apply so far as they are relevant in the particular context; and
- (b) are subject to the need to have regard to other considerations that are also relevant in that context.

(4) The other considerations may, in particular, include-

- (a) the interests of the security of Gibraltar or of the economic well-being of Gibraltar;
- (b) the public interest in preventing or detecting serious crime;
- (c) other considerations which are relevant to-
  - (i) whether the conduct authorised or required by the authorisation or notice is proportionate; or
  - (ii) whether it is necessary to act for a purpose provided for by this Act;

- (d) the requirements of the Gibraltar Constitution Order 2006; and
  - (e) other requirements of public law.
- (5) For the purposes of subsection (2)(b), examples of sensitive information include-
- (a) items subject to legal privilege;
  - (b) any information identifying or confirming a source of journalistic information; and
  - (c) relevant confidential information within the meaning given by section 2.

*Prohibitions against Unlawful Interception*

**Offence of unlawful interception.**

8.(1) A person commits an offence if-

- (a) the person intentionally intercepts a communication in the course of its transmission by means of-
  - (i) a public telecommunication system;
  - (ii) a private telecommunication system; or
  - (iii) a public postal service;
- (b) the interception is carried out in Gibraltar; and
- (c) the person does not have lawful authority to carry out the interception.

(2) But it is not an offence under subsection (1) for a person to intercept a communication in the course of its transmission by means of a private telecommunication system if the person-

- (a) is a person with a right to control the operation or use of the system; or
- (b) has the express or implied consent of such a person to carry out the interception.

(3) Sections 9 and 10 contain provision about-

- (a) the meaning of "interception"; and
- (b) when interception is to be regarded as carried out in Gibraltar.

(4) Section 11 contains provision about when a person has lawful authority to carry out an interception.

(5) For the meaning of the terms used in subsection (1)(a)(i) to (iii), see sections 2 and 3.

(6) A person who is guilty of an offence under subsection (1) is liable-

- (a) on summary conviction in Gibraltar, to a fine up to level 5; or
- (b) on conviction on indictment, to imprisonment for a term not exceeding 2 years or to a fine, or to both.

(7) No proceedings for any offence which is an offence by virtue of this section may be instituted in Gibraltar, except by or with the consent of the Attorney-General.

**Definition of "interception" etc.**

*Interception in relation to telecommunication systems.*

9.(1) For the purposes of this Act, a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if-

- (a) the person does a relevant act in relation to the system; and
- (b) the effect of the relevant act is to make any content of the communication available, at a relevant time, to a person who is not the sender or intended recipient of the communication.

For the meaning of "content" in relation to a communication, see section 3(6).

(2) In this section "relevant act", in relation to a telecommunication system, means-

- (a) modifying, or interfering with, the system or its operation;
- (b) monitoring transmissions made by means of the system; or
- (c) monitoring transmissions made by radiocommunication to or from apparatus that is part of the system.

(3) For the purposes of this section references to modifying a telecommunication system include references to attaching any apparatus to, or otherwise modifying or interfering with-

- (a) any part of the system; or
- (b) any radiocommunication apparatus used for making transmissions to or from apparatus that is part of the system.

(4) In this section "relevant time", in relation to a communication transmitted by means of a telecommunication system, means-

- (a) any time while the communication is being transmitted; and

- (b) any time when the communication is stored in or by the system (whether before or after its transmission).

(5) For the purposes of this section, the cases in which any content of a communication is to be taken to be made available to a person at a relevant time include any case in which any of the communication is diverted or recorded at a relevant time so as to make any content of the communication available to a person after that time.

*Interception in relation to postal services.*

(6) Section 2(2) of the Post Office Act applies for the purposes of determining for the purposes of this Act whether a postal item is in the course of its transmission by means of a postal service as it applies for the purposes of determining for the purposes of that Act whether a postal packet is in course of transmission by post.

*Interception carried out in Gibraltar.*

(7) For the purposes of this Act the interception of a communication is carried out in Gibraltar if, and only if-

- (a) the relevant act or, in the case of a postal item, the interception is carried out by conduct within Gibraltar; and
- (b) the communication is intercepted-
  - (i) in the course of its transmission by means of a public telecommunication system or a public postal service; or
  - (ii) in the course of its transmission by means of a private telecommunication system in a case where the sender or intended recipient of the communication is in Gibraltar.

**Conduct that is not interception.**

10.(1) References in this Act to the interception of a communication do not include references to the interception of any communication broadcast for general reception.

(2) References in this Act to the interception of a communication in the course of its transmission by means of a postal service do not include references to-

- (a) any conduct that takes place in relation only to so much of the communication as consists of any postal data comprised in, included as part of, attached to, or logically associated with a communication (whether by the sender or otherwise) for the purposes of any postal service by means of which it is being or may be transmitted; or

- (b) any conduct, in connection with conduct falling within paragraph (a), that gives a person who is neither the sender nor the intended recipient only so much access to a communication as is necessary for the purpose of identifying such postal data.

For the meaning of "postal data", see section 4.

**Definition of "lawful authority".**

11.(1) For the purposes of this Act, a person has lawful authority to carry out an interception if, and only if-

- (a) the interception is carried out in accordance with an authorisation under Chapter 1 of Part 2;
- (b) the interception is authorised by any of sections 39 to 45; or
- (c) in the case of a communication stored in or by a telecommunication system, the interception-
  - (i) is carried out in accordance with a targeted equipment interference authorisation under Part 4;
  - (ii) is in the exercise of any statutory power that is exercised for the purpose of obtaining information or taking possession of any document or other property; or
  - (iii) is carried out in accordance with a court order made for that purpose.

(2) Conduct which has lawful authority for the purposes of this Act by virtue of subsection (1)(a) or (b) is to be treated as lawful for all other purposes.

(3) Any other conduct which-

- (a) is carried out in accordance with an authorisation under Chapter 1 of Part 2; or
- (b) is authorised by any of sections 39 to 45,

is to be treated as lawful for all purposes.

**Monetary penalties for certain unlawful interceptions.**

12.(1) The competent authority may serve a monetary penalty notice on a person if conditions A and B are met.

(2) A monetary penalty notice is a notice requiring the person on whom it is served to pay to the competent authority a monetary penalty of an amount determined by the competent authority and specified in the notice.

(3) Condition A is that the competent authority considers that-

- (a) the person has intercepted, in Gibraltar, any communication in the course of its transmission by means of a public telecommunication system;
- (b) the person did not have lawful authority to carry out the interception; and
- (c) the person was not, at the time of the interception, making an attempt to act in accordance with an authorisation for interception which might, in the opinion of the competent authority, explain the interception.

(4) Condition B is that the competent authority does not consider that the person has committed an offence under section 8(1).

(5) The amount of a monetary penalty determined by the competent authority under this section must not exceed £50,000.

(6) Schedule 1 (which makes further provision about monetary penalty notices) has effect.

(7) In this section "authorisation for interception" means a targeted interception authorisation or mutual assistance authorisation under Chapter 1 of Part 2.

(8) For the meaning of "interception" and other key expressions used in this section, see sections 9 to 11.

#### **Civil liability for certain unlawful interceptions.**

13.(1) An interception of a communication is actionable at the suit or instance of-

- (a) the sender of the communication; or
- (b) the recipient, or intended recipient, of the communication,

if conditions A to D are met.

(2) Condition A is that the interception is carried out in Gibraltar.

(3) Condition B is that the communication is intercepted-

- (a) in the course of its transmission by means of a private telecommunication system;  
or
- (b) in the course of its transmission, by means of a public telecommunication system, to or from apparatus that is part of a private telecommunication system.

(4) Condition C is that the interception is carried out by, or with the express or implied consent of, a person who has the right to control the operation or use of the private telecommunication system.

(5) Condition D is that the interception is carried out without lawful authority.

(6) For the meaning of "interception" and other key expressions used in this section, see sections 9 to 11.

**Restriction on requesting interception by overseas authorities.**

14.(1) This section applies to a request for any authorities of a country or territory outside Gibraltar to carry out the interception of communications sent by, or intended for, an individual who the person making the request believes will be in Gibraltar at the time of the interception.

(2) A request to which this section applies may not be made by an intercepting authority unless a targeted interception authorisation has been granted under Chapter 1 of Part 2 authorising the person to whom it is addressed to secure the interception of communications sent by, or intended for, that individual.

**Restriction on requesting assistance under mutual assistance agreements etc.**

15.(1) This section applies to a request for assistance in accordance with an international mutual assistance agreement so far as the assistance is in connection with, or in the form of, the interception of communications.

(2) A request to which this section applies may not be made by an intercepting authority to the competent authorities of a country or territory outside Gibraltar unless a mutual assistance authorisation has been granted under Chapter 1 of Part 2 authorising the making of the request.

(3) Subsection (2) does not apply in the case of a request for assistance in connection with, or in the form of, interception of a communication stored in or by a telecommunication system if the request is made-

- (a) in the exercise of a statutory power that is exercised for the purpose of obtaining information or taking possession of any document or other property; or
- (b) in accordance with a court order that is made for that purpose.

(4) In this section-

"international mutual assistance agreement" means an international agreement which-

- (a) relates to the provision of mutual assistance in connection with, or in the form of, the interception of communications; and

- (b) requires the grant of an authorisation, order or equivalent agreement in cases in which assistance is given.

*Prohibition against unlawful obtaining of communications data*

**Offence of unlawfully obtaining communications data.**

16.(1) A relevant person who, without lawful authority, knowingly or recklessly obtains communications data from a telecommunications operator or a postal operator is guilty of an offence.

(2) In this section "relevant person" means a person who holds an office, rank or position with an intercepting authority.

(3) Subsection (1) does not apply to a relevant person who shows that the person acted in the reasonable belief that the person had lawful authority to obtain the communications data.

(4) A person guilty of an offence under this section is liable-

- (a) on summary conviction in Gibraltar-

- (i) to imprisonment for a term not exceeding 12 months; or

- (ii) to a fine,

or to both;

- (b) on conviction on indictment, to imprisonment for a term not exceeding 2 years or to a fine, or to both.

*Restrictions on interference with equipment*

**Mandatory use of equipment interference authorisations.**

17.(1) An intercepting authority may not, for the purpose of obtaining communications, private information or equipment data, engage in conduct which could be authorised by an equipment interference authorisation except under the authority of such an authorisation if-

- (a) the conduct would (unless done under lawful authority) constitute one or more offences under sections 362 to 366A of the Crimes Act 2011 (computer misuse offences); and

- (b) there is a Gibraltar connection.

(2) For the purpose of this section, there is a Gibraltar connection if-

- (a) any of the conduct would take place in Gibraltar (regardless of the location of the equipment which would, or may, be interfered with);

- (b) an intercepting authority believes that any of the equipment which would, or may, be interfered with would, or may, be in Gibraltar at some time while the interference is taking place; or
- (c) a purpose of the interference is to obtain-
  - (i) communications sent by, or to, a person who is, or whom an intercepting authority believes to be, for the time being in Gibraltar;
  - (ii) private information relating to an individual who is, or whom an intercepting authority believes to be, for the time being in Gibraltar; or
  - (iii) equipment data which forms part of, or is connected with, communications or private information falling within sub-paragraph (i) or (ii).

(3) This section does not restrict the ability of an intercepting authority to apply for an equipment interference authorisation in cases where-

- (a) an intercepting authority does not consider that the conduct for which it is seeking an authorisation would (unless done under lawful authority) constitute one or more offences under sections 362 to 366A of the Crimes Act 2011; or
- (b) there is no Gibraltar connection.

(4) In this section-

"communications", "private information" and "equipment data" have the same meaning as in Part 4;

"equipment interference authorisation" means a targeted equipment interference authorisation under Part 4.

## **PART 2**

### **Lawful Interception of Communications**

#### **Chapter 1**

##### **Interception with an Authorisation**

###### *Authorisations under this Chapter*

###### **Authorisations that may be granted under this Chapter.**

18.(1) There are two kinds of authorisations that may be granted under this Chapter-

- (a) targeted interception authorisations (see subsection (2)); and
- (b) mutual assistance authorisations (see subsection (3)).

(2) A targeted interception authorisation authorises or requires the person to whom it is addressed to secure, by any conduct described in the authorisation, any one or more of the following-

- (a) the interception, in the course of their transmission by means of a postal service or telecommunication system, of communications described in the authorisation;
- (b) the obtaining of secondary data from communications transmitted by means of a postal service or telecommunication system and described in the authorisation (see section 19);
- (c) the disclosure, in any manner described in the authorisation, of anything obtained under the authorisation to the person to whom the authorisation is addressed or to any person acting on that person's behalf.

(3) A mutual assistance authorisation is an authorisation which authorises or requires the person to whom it is addressed to secure, by any conduct described in the authorisation, any one or more of the following-

- (a) the making of a request, in accordance with an international mutual assistance agreement, for the provision of any assistance of a kind described in the authorisation in connection with, or in the form of, an interception of communications;
- (b) the provision to the competent authorities of a country or territory outside Gibraltar, in accordance with such an agreement, of any assistance of a kind described in the authorisation in connection with, or in the form of, an interception of communications;
- (c) the disclosure, in any manner described in the authorisation, of anything obtained under the authorisation to the person to whom the authorisation is addressed or to any person acting on that person's behalf.

(4) Authorisations under this Chapter also authorise the following conduct (in addition to the conduct described therein)-

- (a) any conduct which it is necessary to undertake in order to do what is expressly authorised or required by the authorisation, including-
  - (i) the interception of communications not described in the authorisation; and
  - (ii) conduct for obtaining secondary data from such communications;

- (b) any conduct by any person which is conduct in pursuance of a requirement imposed by or on behalf of the person to whom the authorisation is addressed to be provided with assistance in giving effect to the authorisation;
- (c) any conduct for obtaining related systems data from any postal operator or telecommunications operator.

(5) For the purposes of subsection (4)(c)-

"related systems data", in relation to an authorisation, means systems data relating to a relevant communication or to the sender or recipient, or intended recipient, of a relevant communication (whether or not a person); and

"relevant communication", in relation to an authorisation, means-

- (a) any communication intercepted in accordance with the authorisation in the course of its transmission by means of a postal service or telecommunication system; or
- (b) any communication from which secondary data is obtained under the authorisation.

(6) For provision enabling the combination of targeted interception authorisations with certain other authorisations or notices, see Schedule 3.

### **Obtaining secondary data.**

19.(1) This section has effect for the purposes of this Part.

(2) In relation to a communication transmitted by means of a postal service, references to obtaining secondary data from the communication are references to obtaining such data in the course of the transmission of the communication (as to which, see section 9(7)).

(3) In relation to a communication transmitted by means of a telecommunication system, references to obtaining secondary data from the communication are references to obtaining such data-

- (a) while the communication is being transmitted; or
- (b) at any time when the communication is stored in or by the system (whether before or after its transmission).

(4) "Secondary data"-

- (a) in relation to a communication transmitted by means of a postal service, means any data falling within subsection (5);

- (b) in relation to a communication transmitted by means of a telecommunication system, means any data falling within subsection (5) or (6).

(5) The data falling within this subsection is systems data which is comprised in, included as part of, attached to or logically associated with the communication (whether by the sender or otherwise).

(6) The data falling within this subsection is identifying data which-

- (a) is comprised in, included as part of, attached to or logically associated with the communication (whether by the sender or otherwise);
- (b) is capable of being logically separated from the remainder of the communication; and
- (c) if it were so separated, would not reveal anything of what might reasonably be considered to be the meaning (if any) of the communication, disregarding any meaning arising from the fact of the communication or from any data relating to the transmission of the communication.

(7) For the meaning of "systems data" and "identifying data", see section 2.

### **Subject-matter of authorisations.**

20.(1) An authorisation under this Chapter may relate to-

- (a) a particular person or organisation; or
- (b) a single set of premises.

(2) In addition, a targeted interception authorisation may relate to-

- (a) a group of persons who share a common purpose or who carry on, or may carry on, a particular activity;
- (b) more than one person or organisation, or more than one set of premises, where the conduct authorised or required by the authorisation is for the purposes of a single investigation or operation;
- (c) testing or training activities.

(3) In subsection (2)(c) "testing or training activities" means in relation to a targeted interception authorisation-

- (a) the testing, maintenance or development of apparatus, systems or other capabilities relating to the interception of communications in the course of their transmission by means of a telecommunication system or to the obtaining of secondary data from communications transmitted by means of such a system; or

- (b) the training of persons who carry out, or are likely to carry out, such interception or the obtaining of such data.

*Power to grant authorisations*

**Persons who may apply for the grant of an authorisation.**

21. An intercepting authority as defined in section 2 may apply to the competent authority for the grant of an authorisation under this Chapter.

**Power of the competent authority to grant authorisations.**

22.(1) The competent authority may, on an application made by an intercepting authority, grant an authorisation under this Chapter if the competent authority considers that-

- (a) the authorisation is necessary on grounds falling within section 23;
- (b) the conduct authorised by the authorisation is proportionate to what is sought to be achieved by that conduct; and
- (c) satisfactory arrangements made for the purposes of sections 46 and 47 (safeguards relating to disclosure etc.) are in force in relation to the authorisation.

(2) In deciding whether to grant an authorisation the competent authority must consider the matters referred to in subsection (1) with a sufficient degree of care as to ensure that it complies with the duties imposed by section 7 (general duties in relation to privacy).

**Grounds on which authorisations may be granted by the competent authority.**

23.(1) This section has effect for the purposes of this Part.

(2) A targeted interception authorisation is necessary on grounds falling within this section if it is necessary-

- (a) in the interests of the security of Gibraltar;
- (b) for the purpose of preventing or detecting serious crime; or
- (c) in the interests of the economic well-being of Gibraltar so far as those interests are also relevant to the interests of the security of Gibraltar (but see subsection (4)).

(3) A mutual assistance authorisation is necessary on grounds falling within this section if-

- (a) it is necessary for the purpose of giving effect to the provisions of an international mutual assistance agreement; and

- (b) the circumstances appear to the competent authority to be equivalent to those in which the competent authority would grant an authorisation by virtue of subsection (2)(b).

(4) An authorisation may be considered necessary as mentioned in subsection (2)(c) only if the information which it is considered necessary to obtain is information relating to the acts or intentions of persons outside Gibraltar.

(5) An authorisation may not be considered necessary on grounds falling within this section if it is considered necessary only for the purpose of gathering evidence for use in any legal proceedings.

(6) Where the competent authority refuses to grant an authorisation under this Chapter, the competent authority must give an intercepting authority written reasons for the refusal.

(7) Where the competent authority refuses to grant an authorisation under this Chapter, an intercepting authority may appeal the decision to the Supreme Court.

(8) On an appeal under subsection (7), the Supreme Court may-

- (a) confirm the competent authority's decision; or
- (b) make a fresh determination.

(9) In coming to a decision, the Supreme Court must apply the same principles as to be applied by a court on an application for judicial review and consider whether the authorisation satisfies the requirements contained in section 22.

#### *Additional safeguards*

#### **Members of Parliament etc.**

24.(1) Schedule 4 applies where an application is made to the competent authority for the grant of a targeted interception authorisation and the purpose of the authorisation is to authorise or require the interception of communications sent by, or intended for, a Member of Parliament.

#### **Items subject to legal privilege.**

25.(1) Subsections (2) to (5) apply if-

- (a) an application is made to the competent authority by an intercepting authority for an authorisation under this Chapter; and
- (b) the purpose, or one of the purposes, of the authorisation is to authorise or require the interception of items subject to legal privilege.

(2) The application must contain a statement that the purpose, or one of the purposes, of the authorisation is to authorise or require the interception of items subject to legal privilege.

(3) In deciding whether to grant the authorisation, the competent authority must have regard to the public interest in the confidentiality of items subject to legal privilege.

(4) The competent authority may grant the authorisation only if it considers that-

(a) there are exceptional and compelling circumstances that make it necessary to authorise or require the interception of items subject to legal privilege; and

(b) the arrangements made for the purposes of section 46 include specific arrangements for the handling, retention, use and destruction of such items.

(5) But the authorisation may not be granted if it is considered necessary only as mentioned in section 23(2)(c).

(6) For the purposes of subsection (4)(a), there cannot be exceptional and compelling circumstances that make it necessary to authorise or require the interception of items subject to legal privilege unless-

(a) the public interest in obtaining the information that would be obtained by the authorisation outweighs the public interest in the confidentiality of items subject to legal privilege;

(b) there are no other means by which the information may reasonably be obtained; and

(c) in the case of an authorisation considered necessary as mentioned in section 23(2)(b) or (3), obtaining the information is necessary for the purpose of preventing death or significant injury.

(7) Subsections (8) and (9) apply if-

(a) an application is made by an intercepting authority for an authorisation under this Chapter;

(b) the intercepting authority considers that the relevant communications are likely to include items subject to legal privilege; and

(c) subsections (2) to (5) do not apply.

(8) The application must contain-

(a) a statement that the intercepting authority considers that the relevant communications are likely to include items subject to legal privilege; and

- (b) an assessment of how likely it is that the relevant communications will include such items.

(9) The competent authority may grant the authorisation only if it considers that the arrangements made for the purposes of section 46 include specific arrangements for the handling, retention, use and destruction of items subject to legal privilege.

(10) In this section "relevant communications" means, in relation to an authorisation granted under this Chapter, any communications the interception of which is authorised or required by the authorisation.

(11) Subsections (12) and (13) apply if-

- (a) an application is made to the competent authority by an intercepting authority for an authorisation under this Chapter;
- (b) the purpose, or one of the purposes, of the authorisation is to authorise or require the interception of communications that, if they were not made with the intention of furthering a criminal purpose, would be items subject to legal privilege; and
- (c) the intercepting authority considers that the communications ("the targeted communications") are likely to be communications made with the intention of furthering a criminal purpose.

(12) The application must-

- (a) contain a statement that the purpose, or one of the purposes, of the authorisation is to authorise or require the interception of communications that, if they were not made with the intention of furthering a criminal purpose, would be items subject to legal privilege; and
- (b) set out the reasons for believing that the targeted communications are likely to be communications made with the intention of furthering a criminal purpose.

(13) The competent authority may grant the authorisation only if it considers that the targeted communications are likely to be communications made with the intention of furthering a criminal purpose.

### **Confidential journalistic material.**

26.(1) This section applies if-

- (a) an application is made to the competent authority by an intercepting authority for an authorisation under this Chapter; and

- (b) the purpose, or one of the purposes, of the authorisation is to authorise or require the interception of communications which the intercepting authority believes will be communications containing confidential journalistic material.

(2) The application must contain a statement that the purpose, or one of the purposes, of the authorisation sought under this Chapter is to authorise or require the interception of communications which the intercepting authority believes will be communications containing confidential journalistic material.

(3) The competent authority may grant the authorisation only if it considers that the arrangements made for the purposes of section 47 include specific arrangements for the handling, retention, use and destruction of communications containing confidential journalistic material.

(4) For the meaning of "journalistic material" and "confidential journalistic material", see section 5.

#### **Sources of journalistic information.**

27.(1) This section applies if-

- (a) an application is made to the competent authority by an intercepting authority for an authorisation under this Chapter; and
- (b) the purpose, or one of the purposes, of the authorisation is to identify or confirm a source of journalistic information.

(For the meaning of "source of journalistic information", see section 2(1).)

(2) The application must contain a statement that the purpose, or one of the purposes, of the authorisation is to identify or confirm a source of journalistic information.

(3) The competent authority may grant the authorisation only if it considers that the arrangements made for the purposes of section 46 include specific arrangements for the handling, retention, use and destruction of communications that identify sources of journalistic information.

#### *Further provision about authorisations*

#### **Grant of authorisations.**

28. An authorisation granted under this Chapter is subject to section 35 (special rules for certain mutual assistance authorisations).

#### **Requirements that must be met by authorisations.**

29.(1) An authorisation under this Chapter must contain a provision stating whether it is a targeted interception authorisation or a mutual assistance authorisation.

(2) An authorisation granted under this Chapter must be addressed to the person by whom, or on whose behalf, the application for the authorisation was made.

(3) An authorisation that relates to a particular person or organisation, or to a single set of premises, must name or describe that person or organisation or those premises.

(4) An authorisation that relates to a group of persons who share a common purpose or who carry on (or may carry on) a particular activity must-

- (a) describe that purpose or activity; and
- (b) name or describe as many of those persons as it is reasonably practicable to name or describe.

(5) An authorisation that relates to more than one person or organisation, or more than one set of premises, where the conduct authorised or required by the authorisation is for the purposes of a single investigation or operation, must-

- (a) describe the investigation or operation; and
- (b) name or describe as many of those persons or organisations, or as many of those sets of premises, as it is reasonably practicable to name or describe.

(6) An authorisation that relates to any testing or training activities must-

- (a) describe those activities; and
- (b) name or describe as many of the persons within subsection (7) as it is reasonably practicable to name or describe.

"Testing or training activities" has the meaning given by section 20(3).

(7) A person is within this subsection in the case of a targeted interception authorisation if-

- (a) communications from, or intended for, the person will or may be intercepted by an interception authorised or required by the authorisation; or
- (b) secondary data will or may be obtained under the authorisation from communications from, or intended for, the person.

(8) Where an authorisation under this Chapter authorises or requires the interception of communications described in the authorisation, or the obtaining of secondary data from such communications, the authorisation must specify the addresses, numbers, apparatus, or other factors, or combination of factors, that are to be used for identifying the communications.

(9) Any factor, or combination of factors, specified in accordance with subsection (8) must be one that identifies communications which are likely to be or to include-

- (a) communications from, or intended for, any person or organisation named or described in the authorisation; or
- (b) communications originating on, or intended for transmission to, any premises named or described in the authorisation.

(10) In this section any reference to communications from, or intended for, a person or organisation includes communications from, or intended for, anything owned, controlled or operated by that person or organisation.

#### **Duration of authorisations.**

30.(1) An authorisation under this Chapter ceases to have effect at the end of the relevant period (see subsection (2)), unless-

- (a) it is renewed before the end of that period (see section 31); or
- (b) it is cancelled before the end of that period (see section 34).

(2) In this section "the relevant period" means the period of 6 months beginning with-

- (a) the day on which the authorisation was granted; or
- (b) in the case of an authorisation that has been renewed, the day after the day at the end of which the authorisation would have ceased to have effect if it had not been renewed.

#### **Renewal of authorisations.**

31.(1) If the renewal conditions are met, an authorisation granted under this Chapter may be renewed, at any time during the renewal period, by the competent authority on application by an intercepting authority.

(2) The renewal conditions are that the competent authority considers that-

- (a) the authorisation continues to be necessary on any relevant grounds (see subsection (3)); and
- (b) the conduct that would be authorised by the renewed authorisation continues to be proportionate to what is sought to be achieved by that conduct.

(3) "Relevant grounds" means grounds falling within section 23.

(4) "The renewal period" means the period of 30 days ending with the day at the end of which the authorisation would otherwise cease to have effect.

(5) Section 22 (grant of authorisations by the competent authority) applies in relation to a decision to renew an authorisation as it applies in relation to a decision to grant an authorisation.

(6) Sections 24 to 27 (additional safeguards) apply in relation to a decision to renew an authorisation as they apply in relation to a decision to grant an authorisation.

(7) In this section-

"the relevant period" has the same meaning as in section 30.

(8) This section is subject to section 35 (special rules for certain mutual assistance authorisations).

#### **Modification of authorisations.**

32.(1) The provisions of an authorisation granted under this Chapter may be modified at any time by the competent authority on application by an intercepting authority.

(2) The only modifications that may be made under this section are-

- (a) adding, varying or removing the name or description of a person, organisation or set of premises to which the authorisation relates; and
- (b) adding, varying or removing any factor specified in the authorisation in accordance with section 29(8).

(3) But an authorisation may not be modified as mentioned in subsection (2)(a) if it relates only to a particular person or organisation, or to a single set of premises, as mentioned in section 20(1).

(4) In this Chapter-

- (a) a modification adding or varying a name or description as mentioned in subsection (2)(a) is referred to as a "major modification"; and
- (b) any other modification within that subsection is referred to as a "minor modification".

(5) Nothing in this section applies in relation to modifying the provisions of an authorisation in a way which does not affect the conduct authorised or required by it.

#### **Further provision about modifications.**

33.(1) The competent authority may, on application by an intercepting authority, make a modification within subsection (2) only if it considers-

- (a) that the modification is necessary on any relevant grounds (see subsection (3)); and
- (b) that the conduct authorised by the modification is proportionate to what is sought to be achieved by that conduct.

(2) The modifications within this subsection are-

- (a) a major modification adding the name or description of a person, organisation or set of premises to which the authorisation relates; and
- (b) a minor modification adding any factor specified in the authorisation in accordance with section 29(8).

(3) In subsection (1)(a) "relevant grounds" means grounds falling within section 23.

(4) Sections 24 to 27 (additional safeguards) apply in relation to the making of a major modification within subsection (2)(a) above as they apply in relation to the issuing of an authorisation.

(5) In a case where any of sections 24 to 27 applies in relation to the making of a major modification, section 22 applies in relation to the decision to make the modification as it applies in relation to a decision to grant an authorisation, but as if the references in subsection (1)(a) and (b) of that section to the authorisation were references to the modification.

### **Cancellation of authorisations.**

34.(1) The competent authority may, on application by an intercepting authority, cancel an authorisation granted under this Chapter at any time.

(2) If the competent authority considers that-

- (a) an authorisation granted under this Chapter is no longer necessary on any relevant grounds; or
- (b) the conduct authorised by the authorisation is no longer proportionate to what is sought to be achieved by that conduct,

the competent authority must cancel the authorisation.

(3) In subsection (2)(a) "relevant grounds" means grounds falling within section 23.

(4) Where an authorisation is cancelled under this section, the person to whom the authorisation was addressed must, so far as is reasonably practicable, secure that anything in the process of being done under the authorisation stops as soon as possible.

(5) An authorisation that has been cancelled under this section may not be renewed.

(6) See also section 35 (which imposes a duty to cancel mutual assistance authorisations in certain circumstances).

**Special rules for certain mutual assistance authorisations.**

35.(1) For the purposes of this section an authorisation is a "relevant mutual assistance authorisation" if-

- (a) the authorisation is for the purposes of a request for assistance made under an international mutual assistance agreement by the competent authorities of a country or territory outside Gibraltar; and
- (b) either-
  - (i) it appears that the interception subject is outside Gibraltar; or
  - (ii) the interception authorised or required by the authorisation is to take place in relation only to premises outside Gibraltar.

(2) The decision to grant a relevant mutual assistance authorisation must be taken by the competent authority.

(3) In such a case, the authorisation must contain-

- (a) a statement that the authorisation is granted for the purposes of a request for assistance made under an international mutual assistance agreement by the competent authorities of a country or territory outside Gibraltar; and
- (b) whichever of the following statements is applicable-
  - (i) a statement that the interception subject appears to be outside Gibraltar;
  - (ii) a statement that the interception authorised or required by the authorisation is to take place in relation only to premises outside Gibraltar.

(4) A relevant mutual assistance authorisation may be renewed by the competent authority (see section 31).

(5) Where the competent authority renews a relevant mutual assistance authorisation in accordance with subsection (4), the instrument renewing the authorisation must contain-

- (a) a statement that the renewal is for the purposes of a request for assistance made under an international mutual assistance agreement by the competent authorities of a country or territory outside Gibraltar; and
- (b) whichever of the following statements is applicable-

- (i) a statement that the interception subject appears to be outside Gibraltar;
- (ii) a statement that the interception authorised or required by the authorisation is to take place in relation only to premises outside Gibraltar.

(6) Subsection (7) applies in a case where-

- (a) a relevant mutual assistance authorisation-
  - (i) was granted containing the statement set out in subsection (3)(b)(i); or
  - (ii) has been renewed by an instrument containing the statement set out in subsection (5)(b)(i), and
- (b) the last renewal (if any) of the authorisation was a renewal by the competent authority in accordance with subsection (4).

(7) If the competent authority believes that the person, group or organisation named or described in the authorisation as the interception subject is in Gibraltar, that person must cancel the authorisation under section 34.

(8) In this section "the interception subject", in relation to an authorisation, means the person, group of persons or organisation to which the authorisation relates.

#### *Implementation of authorisations*

#### **Implementation of authorisations.**

36.(1) This section applies to authorisations granted under this Chapter.

(2) In giving effect to an authorisation to which this section applies, the person to whom it is addressed ("the intercepting authority" see section 2) may (in addition to acting alone) act through, or together with, such other persons as the intercepting authority may require (whether under subsection (3) or otherwise) to provide the authority with assistance in giving effect to the authorisation.

(3) For the purpose of requiring any person to provide assistance in relation to an authorisation to which this section applies, the intercepting authority may-

- (a) serve a copy of the authorisation on any person who the intercepting authority considers may be able to provide such assistance; or
- (b) make arrangements for the service of a copy of the authorisation on any such person.

(4) A copy of an authorisation may be served under subsection (3) on a person outside Gibraltar for the purpose of requiring the person to provide such assistance in the form of conduct outside Gibraltar.

(5) For the purposes of this Act, the provision of assistance in giving effect to an authorisation to which this section applies includes any disclosure to the intercepting authority, or to persons acting on behalf of the intercepting authority, of anything obtained under the authorisation.

(6) References in this section and sections 37 and 38 to the service of a copy of an authorisation include-

- (a) the service of a copy of one or more schedules contained in the authorisation with the omission of the remainder of the authorisation; and
- (b) the service of a copy of the authorisation with the omission of any schedule contained in the authorisation.

### **Service of authorisations.**

37.(1) This section applies to the service of authorisations under section 36(3).

(2) A copy of the authorisation must be served in such a way as to bring the contents of the authorisation to the attention of the person who the intercepting authority considers may be able to provide assistance in relation to it.

(3) A copy of an authorisation may be served on a person outside Gibraltar in any of the following ways (as well as by electronic or other means of service)-

- (a) by serving it at the person's principal office within Gibraltar or, if the person has no such office in Gibraltar, at any place in Gibraltar where the person carries on business or conducts activities;
- (b) if the person has specified an address in Gibraltar as one at which the person, or someone on the person's behalf, will accept service of documents of the same description as a copy of an authorisation, by serving it at that address;
- (c) by making it available for inspection (whether to the person or to someone acting on the person's behalf) at a place in Gibraltar (but this is subject to subsection (4)).

(4) A copy of an authorisation may be served on a person outside Gibraltar in the way mentioned in subsection (3)(c) only if-

- (a) it is not reasonably practicable for a copy to be served by any other means (whether as mentioned in subsection (3)(a) or (b) or otherwise); and
- (b) the intercepting authority takes such steps as the authority considers appropriate for the purpose of bringing the contents of the authorisation, and the availability of a copy for inspection, to the attention of the person.

(5) The steps mentioned in subsection (4)(b) must be taken as soon as reasonably practicable after the copy of the authorisation is made available for inspection.

(6) In this section "the intercepting authority" has the same meaning as in section 36.

**Duty of operators to assist with implementation.**

38.(1) A relevant operator that has been served with a copy of an authorisation to which section 36 applies by (or on behalf of) the intercepting authority must take all steps for giving effect to the authorisation that are notified to the relevant operator by (or on behalf of) the intercepting authority.

This is subject to subsection (4).

(2) In this section-

"relevant operator" means a postal operator or a telecommunications operator;

"the intercepting authority" has the same meaning as in section 36.

(3) Subsection (1) applies whether or not the relevant operator is in Gibraltar.

(4) The relevant operator is not required to take any steps which it is not reasonably practicable for the relevant operator to take.

(5) In determining for the purposes of subsection (4) whether it is reasonably practicable for a relevant operator outside Gibraltar to take any steps in a country or territory outside Gibraltar for giving effect to an authorisation, the matters to be taken into account include the following-

- (a) any requirements or restrictions under the law of that country or territory that are relevant to the taking of those steps; and
- (b) the extent to which it is reasonably practicable to give effect to the authorisation in a way that does not breach any of those requirements or restrictions.

(6) A person who knowingly fails to comply with subsection (1) is guilty of an offence and liable-

(a) on summary conviction in Gibraltar-

- (i) to imprisonment for a term not exceeding 12 months; or
- (ii) to a fine,

or to both;

(b) on conviction on indictment, to imprisonment for a term not exceeding 2 years or to a fine, or to both.

(7) The duty imposed by subsection (1) is enforceable (whether or not the person is in Gibraltar) by civil proceedings by the Attorney-General for an injunction or for any other appropriate relief.

## **Chapter 2**

### **Other Forms of Lawful Interception**

#### *Interception with consent*

##### **Interception with the consent of the sender or recipient.**

39.(1) The interception of a communication is authorised by this section if the sender and the intended recipient of the communication have each consented to its interception.

(2) The interception of a communication is authorised by this section if-

- (a) the communication is one sent by, or intended for, a person who has consented to the interception; and
- (b) surveillance by means of that interception has been authorised under Part 5 of this Act.

#### *Interception for administrative or enforcement purposes*

##### **Interception by providers of postal or telecommunications services.**

40.(1) The interception of a communication is authorised by this section if the interception is carried out-

- (a) by, or on behalf of, a person who provides a postal service or a telecommunications service; and
- (b) for any of the purposes in subsection (2).

(2) The purposes referred to in subsection (1) are purposes relating to-

- (a) the provision or operation of the service;
- (b) the enforcement, in relation to the service, of any enactment relating to-
  - (i) the use of postal or telecommunications services; or
  - (ii) the content of communications transmitted by means of such services;

- (c) the provision of services or facilities aimed at preventing or restricting the viewing or publication of the content of communications transmitted by means of postal or telecommunications services.

(3) A reference in this section to anything carried out for purposes relating to the provision or operation of a telecommunications service includes, among other things, a reference to anything done for the purposes of identifying, combating or preventing anything which could affect-

- (a) any telecommunication system by means of which the service is provided; or
- (b) any apparatus attached to such a system.

**Interception by businesses etc. for monitoring and record-keeping purposes.**

41.(1) Conduct is authorised by this section if it is authorised by regulations made under subsection (2).

(2) The Minister may by regulations authorise conduct of a description specified in the regulations if that conduct appears to the Minister to constitute a legitimate practice reasonably required for the purpose, in connection with the carrying on of any relevant activities (see subsection (4)), of monitoring or keeping a record of-

- (a) communications by means of which transactions are entered into in the course of the relevant activities; or
- (b) other communications relating to the relevant activities or taking place in the course of the carrying on of those activities.

(3) But nothing in any regulations under subsection (2) may authorise the interception of any communication except in the course of its transmission using apparatus or services provided by or to the person carrying on the relevant activities for use (whether wholly or partly) in connection with those activities.

(4) In this section "relevant activities" means-

- (a) any business;
- (b) any activities of a government department;
- (c) any activities of a public authority; and
- (d) any activities of any person or office holder on whom functions are conferred by or under any enactment.

**Postal services: interception for enforcement purposes.**

42.(1) The interception of a communication in the course of its transmission by means of a postal service is authorised by this section if it is carried out by a police officer, customs officer or a postal operator, as applied by virtue of-

- (a) the Post Office Act or the Import and Exports Act, 1986; or
- (b) any another enactment.

(2) The interception of a communication in the course of its transmission by means of a postal service is authorised by this section if it is carried out under paragraph 9 of Schedule 10 to the Terrorism Act 2018(port and border controls).

**Interception by the Gibraltar Regulatory Authority (“GRA”) in connection with radiocommunication.**

43.(1) Conduct falling within subsection (2) is authorised by this section if it is carried out by the GRA for purposes connected with a relevant matter (see subsection (3)).

(2) The conduct referred to in subsection (1) is-

- (a) the interception of a communication in the course of its transmission by means of a telecommunication system;
- (b) the obtaining, by or in connection with the interception, of information about the sender or recipient, or intended recipient, of the communication (whether or not a person);
- (c) the disclosure of anything obtained by conduct falling within paragraph (a) or (b).

(3) Each of the following is a relevant matter for the purposes of subsection (1)-

- (a) the grant of radiocommunication licences under the Communications Act 2006 ("the 2006 Act");
- (b) the prevention or detection of anything which constitutes interference with radiocommunication;
- (c) the enforcement of-
  - (i) sections 60 to 66 of the 2006 Act; or
  - (ii) any enactment not falling within sub-paragraph (i) that relates to interference with radiocommunication.

(4) In this section-

"interference", in relation to radiocommunication, has the same meaning as in the Communications Act 2006 (see section 62(3) of that Act);

"radiocommunication" has the same meaning as in the Communications Act 2006 (see section 2 of that Act).

*Interception taking place in certain institutions*

**Interception in prisons.**

44.(1) Conduct taking place in a prison is authorised by this section if it is conduct in exercise of any power conferred by or under regulations made under section 71 of the Prison Act 2011.

(2) In this section "prison" means any place declared by order under section 3 of the Prison Act 2011 to be a prison or part of a prison.

*Interception in accordance with overseas requests*

**Interception in accordance with overseas requests.**

45.(1) The interception of a communication in the course of its transmission by means of a telecommunication system is authorised by this section if conditions A to D are met.

(2) Condition A is that the interception-

(a) is carried out by or on behalf of a telecommunications operator; and

(b) relates to the use of a telecommunications service provided by the telecommunications operator.

(3) Condition B is that the interception is carried out in response to a request made in accordance with a relevant international agreement by the competent authorities of a country or territory outside Gibraltar.

In this subsection "relevant international agreement" means an international agreement which applies to Gibraltar.

(4) Condition C is that the interception is carried out for the purpose of obtaining information about the communications of an individual-

(a) who is outside Gibraltar; or

(b) who each of the following persons believes is outside Gibraltar-

(i) the person making the request;

- (ii) the person carrying out the interception.

(5) Condition D is that any further conditions specified in regulations made by the Minister for the purposes of this section are met.

### **Chapter 3**

#### **Other Provisions about Interception**

*Restrictions on use or disclosure of material obtained under authorisations etc.*

#### **Safeguards relating to retention and disclosure of material.**

46.(1) The competent authority must ensure, in relation to every authorisation granted by it under Chapter 1, that arrangements are in force for securing that the requirements of subsections (2) and (5) are met in relation to the material obtained under the authorisation.

This is subject to subsection (9).

(2) The requirements of this subsection are met in relation to the material obtained under an authorisation if each of the following is limited to the minimum that is necessary for the authorised purposes (see subsection (3))-

- (a) the number of persons to whom any of the material is disclosed or otherwise made available;
- (b) the extent to which any of the material is disclosed or otherwise made available;
- (c) the extent to which any of the material is copied;
- (d) the number of copies that are made.

(3) For the purposes of this section something is necessary for the authorised purposes if, and only if-

- (a) it is, or is likely to become, necessary on any of the grounds falling within section 23 on which an authorisation under Chapter 1 of this Part may be necessary;
- (b) it is necessary for facilitating the carrying out of any functions under this Act of the Minister or the person to whom the authorisation is or was addressed;
- (c) it is necessary for facilitating the carrying out of any functions of the competent authority under or in relation to this Act; or
- (d) it is necessary to ensure that a person ("P") who is conducting a criminal prosecution has the information P needs to determine what is required of P by P's duty to secure the fairness of the prosecution.

(4) The arrangements for the time being in force under this section for securing that the requirements of subsection (2) are met in relation to the material obtained under the authorisation must include arrangements for securing that every copy made of any of that material is stored, for so long as it is retained, in a secure manner.

(5) The requirements of this subsection are met in relation to the material obtained under an authorisation if every copy made of any of that material (if not destroyed earlier) is destroyed as soon as there are no longer any relevant grounds for retaining it (see subsection (6)).

(6) For the purposes of subsection (5), there are no longer any relevant grounds for retaining a copy of any material if, and only if-

- (a) its retention is not necessary, or not likely to become necessary, on any of the grounds falling within section 19 on which an authorisation under Chapter 1 of this Part may be necessary; and
- (b) its retention is not necessary for any of the purposes mentioned in paragraphs (b) to (d) of subsection (3) above.

(7) Where-

- (a) a communication which has been intercepted in accordance with an authorisation granted under Chapter 1 is retained, following its examination, for purposes other than the destruction of the communication; and
- (b) it is a communication that contains confidential journalistic material or identifies a source of journalistic information,

the person to whom the authorisation is addressed must inform the competent authority as soon as is reasonably practicable.

(8) Subsection (9) applies if-

- (a) any material obtained under the authorisation has been handed over to any overseas authorities; or
- (b) a copy of any such material has been given to any overseas authorities.

(9) To the extent that the requirements of subsections (2) and (5) relate to any of the material mentioned in subsection (8)(a), or to the copy mentioned in subsection (8)(b), the arrangements made for the purposes of this section are not required to secure that those requirements are met (see instead section 47).

(10) In this section-

"copy", in relation to material obtained under an authorisation, means any of the following (whether or not in documentary form)-

- (a) any copy, extract or summary of the material which identifies the material as having been obtained under the authorisation; and
- (b) any record which-
  - (i) refers to any interception or to the obtaining of any material; and
  - (ii) is a record of the identities of the persons to or by whom the material was sent, or to whom the material relates,

and "copied" is to be read accordingly;

"overseas authorities" means authorities of a country or territory outside Gibraltar.

**Safeguards relating to disclosure of material overseas.**

47.(1) The competent authority must ensure, in relation to every authorisation granted by it under Chapter 1, that arrangements are in force for securing that-

- (a) any material obtained under the authorisation is handed over to overseas authorities only if the requirements of subsection (2) are met; and
- (b) copies of any such material are given to overseas authorities only if those requirements are met.

(2) The requirements of this subsection are met in the case of an authorisation if it appears to the competent authority-

- (a) that requirements corresponding to the requirements of section 46(2) and (5) will apply, to such extent (if any) as the competent authority considers appropriate, in relation to any of the material which is handed over, or any copy of which is given, to the authorities in question; and
- (b) that restrictions are in force which would prevent, to such extent (if any) as the competent authority considers appropriate, the doing of anything in, for the purposes of or in connection with any proceedings outside Gibraltar which would result in a prohibited disclosure.

(3) In subsection (2)(b) "prohibited disclosure" means a disclosure which, if made in Gibraltar, would breach the prohibition in section 49(1).

(4) In this section-

"copy" has the same meaning as in section 46;

"overseas authorities" means authorities of a country or territory outside Gibraltar.

**Additional safeguards for items subject to legal privilege.**

48.(1) This section applies where an item subject to legal privilege which has been intercepted in accordance with an authorisation granted under Chapter 1 is retained, following its examination, for purposes other than the destruction of the item.

(2) The person to whom the authorisation is addressed must inform the competent authority of the retention of the item as soon as is reasonably practicable.

(3) Unless the competent authority considers that subsection (5) applies to the item, it must-

- (a) direct that the item is destroyed; or
- (b) impose one or more conditions as to the use or retention of that item.

(4) If the competent authority considers that subsection (5) applies to the item, it may nevertheless impose such conditions under subsection (3)(b) as it considers necessary for the purpose of protecting the public interest in the confidentiality of items subject to legal privilege.

(5) This subsection applies to an item subject to legal privilege if-

- (a) the public interest in retaining the item outweighs the public interest in the confidentiality of items subject to legal privilege; and
- (b) retaining the item is necessary in the interests of the security of Gibraltar or for the purpose of preventing death or significant injury.

(6) The competent authority-

- (a) may require an affected party to make representations about how it should exercise any function under subsection (3); and
- (b) must have regard to any such representations made by an affected party (whether or not as a result of a requirement imposed under paragraph (a)).

(7) For the purposes of subsection (6) the person to whom the authorisation is or was addressed is an “affected party”.

**Exclusion of matters from legal proceedings etc.**

49.(1) No evidence may be adduced, question asked, assertion or disclosure made or other thing done in, for the purposes of or in connection with any legal proceedings or Inquiries Act 2024 proceedings which (in any manner)-

- (a) discloses, in circumstances from which its origin in interception-related conduct may be inferred-

- (i) any content of an intercepted communication; or
- (ii) any secondary data obtained from a communication; or
- (b) tends to suggest that any interception-related conduct has or may have occurred or may be going to occur.

This is subject to Schedule 2 (exceptions).

(2) "Interception-related conduct" means-

- (a) conduct by a person within subsection (3) that is, or in the absence of any lawful authority would be, an offence under section 8(1) (offence of unlawful interception);
- (b) a breach of the prohibition imposed by section 14 (restriction on requesting interception by overseas authorities);
- (c) a breach of the prohibition imposed by section 15 (restriction on requesting assistance under mutual assistance agreements etc.);
- (d) the making of an application by any person for an authorisation, or the grant of an authorisation, under Chapter 1 of this Part;
- (e) the imposition of any requirement on any person to provide assistance in giving effect to an authorisation granted under Chapter 1.

(3) The persons referred to in subsection (2)(a) are-

- (a) any person who is an intercepting authority (see section 21);
- (b) any person holding office under the Crown in right of the Government of Gibraltar;
- (c) any customs officer or police officer;
- (d) any person employed by, or for the purposes of, the Royal Gibraltar Police or HM Customs Gibraltar;
- (e) any postal operator or telecommunications operator;
- (f) any person employed or engaged for the purposes of the business of a postal operator or telecommunications operator.

(4) In this section-

"Inquiries Act 2024 proceedings" means proceedings of an inquiry under the Inquiries Act 2024;

"intercepted communication" means any communication intercepted in the course of its transmission by means of a postal service or telecommunication system.

**Duty not to make unauthorised disclosures.**

50.(1) A person to whom this section applies must not make an unauthorised disclosure to another person.

- (2) A person makes an unauthorised disclosure for the purposes of this section if-
- (a) the person discloses any of the matters within subsection (4) in relation to an authorisation under Chapter 1 of this Part; and
  - (b) the disclosure is not an excepted disclosure (see section 51).
- (3) This section applies to the following persons-
- (a) any person who is an intercepting authority (see section 21);
  - (b) any person holding office under the Crown in right of the Government of Gibraltar;
  - (c) any person employed by, or for the purposes of, the Royal Gibraltar Police or HM Customs Gibraltar;
  - (d) any postal operator or telecommunications operator;
  - (e) any person employed or engaged for the purposes of the business of a postal operator or telecommunications operator;
  - (f) any person to whom any of the matters within subsection (4) have been disclosed in relation to an authorisation mentioned in subsection (2)(a).
- (4) The matters referred to in subsection (2)(a) are-
- (a) the existence or contents of the authorisation;
  - (b) the details of the grant of the authorisation or of any renewal or modification of the authorisation;
  - (c) the existence or contents of any requirement to provide assistance in giving effect to the authorisation;
  - (d) the steps taken in pursuance of the authorisation or of any such requirement;
  - (e) any of the material obtained under the authorisation.

**Section 50: meaning of "excepted disclosure".**

51.(1) For the purposes of section 50 a disclosure made in relation to an authorisation is an "excepted disclosure" if it falls within any of the Heads set out in-

- (a) subsection (2) (disclosures authorised by authorisation etc.);
- (b) subsection (4) (oversight bodies);
- (c) subsection (5) (legal advisers);
- (d) subsection (8) (disclosures of a general nature).

(2) Head 1 is-

- (a) a disclosure authorised by the authorisation;
- (b) a disclosure authorised by the person to whom the authorisation is or was addressed or under any arrangements made by that person for the purposes of this section;
- (c) a disclosure authorised by the terms of any requirement to provide assistance in giving effect to the authorisation (including any requirement for disclosure imposed by virtue of section 36(5)).

(3) But subsection (2)(b) does not apply in the case of a mutual assistance authorisation that is or was addressed to a person falling within section 21 who are competent authorities of overseas countries or territories.

(4) Head 2 is-

- (a) in the case of an authorisation under Chapter 1 of this Part, a disclosure made to, or authorised by, the competent authority;
- (b) a disclosure made to an intercepting authority for the purposes of facilitating the carrying out of any of its functions;

(5) Head 3 is-

- (a) a disclosure made by a legal adviser-
  - (i) in contemplation of, or in connection with, any legal proceedings; and
  - (ii) for the purposes of those proceedings;
- (b) a disclosure made-

- (i) by a professional legal adviser ("L") to L's client or a representative of L's client; or
- (ii) by L's client, or by a representative of L's client, to L,

in connection with the giving, by L to L's client, of advice about the effect of the relevant provisions (see subsection (7)).

(6) But a disclosure within Head 3 is not an excepted disclosure if it is made with the intention of furthering a criminal purpose.

(7) In subsection (5)(b) "the relevant provisions" means in the case of an authorisation under Chapter 1 of this Part, the provisions of this Part.

(8) Head 4 is-

(a) a disclosure that-

- (i) is made by a postal operator or a telecommunications operator in accordance with a requirement imposed by regulations made by the Minister; and
- (ii) consists of statistical information of a description specified in the regulations;

(b) a disclosure of information that does not relate to any particular authorisation under Chapter 1 of this Part but relates to any such authorisations in general.

(9) Nothing in this section affects the operation of section 49 (which, among other things, prohibits the making of certain disclosures in, for the purposes of or in connection with legal proceedings).

#### **Offence of making unauthorised disclosures.**

52.(1) A person who fails to comply with section 50(1) commits an offence.

(2) A person who is guilty of an offence under this section is liable-

(a) on summary conviction-

- (i) to imprisonment for a term not exceeding 12 months, or
- (ii) to a fine,

or to both;

(b) on conviction on indictment-

- (i) to imprisonment for a term not exceeding 5 years, or
- (ii) to a fine,

or to both.

(3) In proceedings against any person for an offence under this section in respect of any disclosure, it is a defence for the person to show that the person could not reasonably have been expected, after first becoming aware of the matter disclosed, to take steps to prevent the disclosure.

### *Interpretation*

#### **Part 2: interpretation.**

53.(1) In this Part-

"intercepting authority" is to be read in accordance with section 21;

"international mutual assistance agreement" has the meaning given by section 15(4);

"mutual assistance authorisation" has the meaning given by section 18(3);

"secondary data" has the meaning given by section 19, and references to obtaining secondary data from a communication are to be read in accordance with that section.

(2) See also-

section 2 (general definitions);

section 3 (telecommunications definitions);

section 4 (postal definitions);

section 5 (general definitions: "journalistic material" etc.).

## **PART 3**

### **Authorisations for Obtaining Communications Data**

#### *Targeted authorisations for obtaining data*

#### **Power to grant authorisations.**

54.(1) Subsection (2) applies if the competent authority, on application made by an intercepting authority, considers that-

- (a) it is necessary to obtain communications data for a purpose falling within subsection (7);
- (b) it is necessary for the intercepting authority to obtain the data-
  - (i) for the purposes of a specific investigation or a specific operation; or
  - (ii) for the purposes of testing, maintaining or developing equipment, systems or other capabilities relating to the availability or obtaining of communications data; and
- (c) the conduct authorised by the authorisation is proportionate to what is sought to be achieved.

(2) The competent authority may grant an authorisation authorising the intercepting authority to engage in any conduct which-

- (a) is for the purpose of obtaining the data from any person; and
- (b) relates to-
  - (i) a telecommunication system; or
  - (ii) data derived from a telecommunication system.

(3) Subsections (1) and (2) are subject to-

- (a) section 55 (restrictions in relation to internet connection records); and
- (b) section 59 (further provisions on grant of authorisations).

(4) Authorised conduct may, in particular, consist of an authorised officer (see section 64)-

- (a) obtaining the communications data themselves from any person or telecommunication system;
- (b) asking any person whom the authorised officer believes is, or may be, in possession of the communications data or capable of obtaining it-
  - (i) to obtain the data (if not already in possession of it); and
  - (ii) to disclose the data (whether already in the person's possession or subsequently obtained by that person) to a person identified by, or in accordance with, the authorisation; or
- (c) requiring by notice a telecommunications operator whom the authorised officer believes is, or may be, in possession of the communications data or capable of obtaining it-

- (i) to obtain the data (if not already in possession of it); and
- (ii) to disclose the data (whether already in the operator's possession or subsequently obtained by the operator) to a person identified by, or in accordance with, the authorisation.

(5) An authorisation-

- (a) may relate to data whether or not in existence at the time of the authorisation;
- (b) may authorise the obtaining or disclosure of data by a person who is not an authorised officer, or any other conduct by such a person, which enables or facilitates the obtaining of the communications data concerned; and
- (c) may, in particular, require a telecommunications operator who controls or provides a telecommunication system to obtain or disclose data relating to the use of a telecommunications service provided by another telecommunications operator in relation to that system.

(6) An authorisation-

- (a) may not authorise any conduct consisting in the interception of communications in the course of their transmission by means of a telecommunication system; and
- (b) may not authorise an authorised officer to ask or require, in the circumstances mentioned in subsection (4)(b) or (c), a person to disclose the data to any person other than-
  - (i) an authorised officer; or
  - (ii) an officer of the same intercepting authority as an authorised officer.

(7) It is necessary to obtain communications data for a purpose falling within this subsection if it is necessary to obtain the data-

- (a) in the interests of the security of Gibraltar;
- (b) for the applicable crime purpose;
- (c) in the interests of the economic well-being of Gibraltar so far as those interests are also relevant to the interests of the security of Gibraltar;
- (d) in the interests of public safety;

- (e) for the purpose 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;
  - (f) to assist investigations into alleged miscarriages of justice; or
  - (g) where a person ("P") has died or is unable to identify themselves because of a physical or mental condition-
    - (i) to assist in identifying P; or
    - (ii) to obtain information about P's next of kin or other persons connected with P or about the reason for P's death or condition.
- (8) In subsection 7(b), “the applicable crime purpose” means-
- (a) where the communication data is wholly or partly events data, the purpose of preventing or detecting serious crime;
  - (b) in any other case, the purpose of preventing or detecting crime or of preventing disorder.
- (9) The fact that the communications data which would be obtained in pursuance of an authorisation relates to the activities in Gibraltar of a trade union is not, of itself, sufficient to establish that it is necessary to obtain the data for a purpose falling within subsection (7).
- (10) See-
- (a) section 62 for the way in which this Part applies to postal operators and postal services;
  - (b) section 64 for the meaning of “serious crime”.

**Restrictions in relation to internet connection records.**

55.(1) The competent authority may not, on the application of an intercepting authority, grant an authorisation for the purpose of obtaining data which is, or can only be obtained by processing, an internet connection record unless condition A, B or C is met.

(2) Condition A is that the competent authority considers that it is necessary, for a purpose falling within section 54(7), to obtain the data to identify which person or apparatus is using an internet service where-

- (a) the service and time of use are already known; but
- (b) the identity of the person or apparatus using the service is not known.

(3) Condition B is that-

- (a) the purpose for which the data is to be obtained falls within section 54(7) but is not the purpose of preventing or detecting serious crime mentioned in section 54(8)(a) or the purpose of preventing or detecting crime mentioned in section 54(8)(b); and
- (b) the competent authority considers that it is necessary to obtain the data to identify-
  - (i) which internet communications service is being used, and when and how it is being used, by a person or apparatus whose identity is already known;
  - (ii) where or when a person or apparatus whose identity is already known is obtaining access to, or running, a computer file or computer program which wholly or mainly involves making available, or acquiring, material whose possession is a crime; or
  - (iii) which internet service is being used, and when and how it is being used, by a person or apparatus whose identity is already known.

(4) Condition C is that-

- (a) either –
  - (i) the purpose for which the data is to be obtained is the purpose of preventing or detecting serious crime mentioned in section 54(8)(a); or
  - (ii) the purpose for which the data is to be obtained is the purpose of preventing or detecting crime mentioned in section 54(8)(b) and the crime to be prevented or detected is serious crime, and;
- (b) the competent authority considers that it is necessary to obtain the data to identify-
  - (i) which internet communications service is being used, and when and how it is being used, by a person or apparatus whose identity is already known;
  - (ii) where or when a person or apparatus whose identity is already known is obtaining access to, or running, a computer file or computer program which wholly or mainly involves making available, or acquiring, material whose possession is a crime; or
  - (iii) which internet service is being used, and when and how it is being used, by a person or apparatus whose identity is already known.

(5) In this Act "internet connection record" means communications data which-

- (a) may be used to identify, or assist in identifying, a telecommunications service to which a communication is transmitted by means of a telecommunication system

for the purpose of obtaining access to, or running, a computer file or computer program; and

- (b) comprises data generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of the communication (whether or not a person).

**Procedure for authorisations under this Part.**

56.(1) An authorisation granted under this Part must specify-

- (a) the intercepting authority the authorisation is being granted to;
- (b) the matters falling within section 54(7) by reference to which it is granted;
- (c) the conduct that is authorised;
- (d) the data or description of data to be obtained; and
- (e) the persons or descriptions of persons to whom the data is to be, or may be, disclosed or how to identify such persons.

(2) An authorisation which imposes requirements on a telecommunications operator must also specify-

- (a) the operator concerned; and
- (b) the nature of the requirements that are to be imposed.

(3) An authorisation must be applied for, and granted, in writing or (if not in writing) in a manner that produces a record of its having been applied for or granted.

**Duration and cancellation of authorisations.**

57.(1) An authorisation ceases to have effect at the end of the period of one month beginning with the date on which it is granted.

(2) An authorisation may be renewed at any time before the end of that period by the grant of a further authorisation.

(3) Subsection (1) has effect in relation to a renewed authorisation as if the period of one month mentioned in that subsection did not begin until the end of the period of one month applicable to the authorisation that is current at the time of the renewal.

(4) The competent authority who granted the authorisation-

- (a) may cancel it at any time on application by an intercepting authority; and

- (b) must cancel it if it considers that the requirements of this Part would not be satisfied in relation to issuing an equivalent new authorisation.

**Duties of telecommunications operators in relation to authorisations.**

58.(1) It is the duty of a telecommunications operator on whom a requirement is imposed by an authorisation to comply with that requirement.

(2) It is the duty of a telecommunications operator who is obtaining or disclosing communications data, in response to a request or requirement for the data in pursuance of an authorisation, to obtain or disclose the data in a way that minimises the amount of data that needs to be processed for the purpose concerned.

(3) A person who is under a duty by virtue of subsection (1) or (2) is not required to take any steps in pursuance of that duty which it is not reasonably practicable for that person to take.

(4) The duty imposed by subsection (1) or (2) is enforceable by civil proceedings by the Attorney-General for an injunction or for any other appropriate relief.

**Further provisions on grant of authorisations.**

59.(1) This section applies to all authorisations granted under this Part.

(2) An intercepting authority is not required to give notice of the application for an authorisation to-

- (a) any person to whom the authorisation relates; or
- (b) that person's legal representatives.

(3) The competent authority may grant the authorisation if, and only if, the competent authority considers that there are reasonable grounds for considering that the requirements of this Part are satisfied in relation to the authorisation.

(4) In considering whether the requirements of an authorisation in relation to the obtaining of communications data for the purpose of identifying or confirming a source of journalistic information are satisfied, the competent authority must, in particular, have regard to-

- (a) the public interest in protecting a source of journalistic information; and
- (b) the need for there to be another overriding public interest before an intercepting authority seeks to identify or confirm a source of journalistic information.

(5) Where, on an application under this section, the competent authority refuses to grant the authorisation, the competent authority may dismiss the application.

*Further and supplementary provision*

**Lawfulness of conduct authorised by an authorisation granted under this Part.**

60.(1) Conduct is lawful for all purposes if-

- (a) it is conduct in which any person is authorised to engage by the authorisation; and
- (b) the conduct is in accordance with, or in pursuance of, the authorisation.

(2) A person (whether or not the person so authorised or required) is not to be subject to any civil liability in respect of conduct that-

- (a) is incidental to, or is reasonably undertaken in connection with, conduct that is lawful by virtue of subsection (1); and
- (b) is not itself conduct for which an authorisation-
  - (i) is capable of being granted under this Act; and
  - (ii) might reasonably have been expected to have been sought in the case in question.

**Offence of making unauthorised disclosure.**

61.(1) It is an offence for a telecommunications operator, or any person employed or engaged for the purposes of the business of a telecommunications operator, to disclose, without reasonable excuse, to any person the existence of-

- (a) any requirement imposed on the operator by virtue of this Part to disclose communications data relating to that person; or
- (b) any request made in pursuance of an authorisation for the operator to disclose such data.

(2) For the purposes of subsection (1), it is, in particular, a reasonable excuse if the disclosure is made with the permission of the intercepting authority which is seeking to obtain the data from the operator (whether the permission is contained in the authorisation requiring the operator to disclose the data or otherwise).

(3) A person guilty of an offence under this section is liable-

- (a) on summary conviction-
  - (i) to imprisonment for a term not exceeding 12 months, or
  - (ii) to a fine,

or to both;

(b) on conviction on indictment-

(i) to imprisonment for a term not exceeding 2 years, or

(ii) to a fine,

or to both.

### **Application of Part 3 to postal operators and postal services.**

62.(1) This Part applies to postal operators and postal services as it applies to telecommunications operators and telecommunications services.

(2) In its application by virtue of subsection (1), this Part has effect as if-

(a) any reference to a telecommunications operator were a reference to a postal operator;

(b) any reference to a telecommunications service were a reference to a postal service;

(c) any reference to a telecommunication system were a reference to a postal service;

(d) sections 54(3)(a) and 55 were omitted; and

(e) the reference in section 54(8)(a) to events data were a reference to anything within paragraph (a) or (b) of the definition of “communications data” in section 4(3).

### **Extra-territorial application of Part 3.**

63.(1) An authorisation may relate to conduct outside Gibraltar and persons outside Gibraltar.

(2) Where such an authorisation is served on a person outside Gibraltar, the authorisation may be served on the person in any of the following ways (as well as by electronic or other means of service)-

(a) by delivering it to the person's principal office within Gibraltar or, if the person has no such office in Gibraltar, to any place in Gibraltar where the person carries on business or conducts activities;

(b) if the person has specified an address in Gibraltar as one at which the person, or someone on the person's behalf, will accept documents of the same description as an authorisation, by delivering it to that address;

(c) by notifying the person by such other means as the authorised officer considers appropriate (which may include notifying the person orally).

(3) In determining for the purposes of subsection (3) of section 58 whether it is reasonably practicable for a telecommunications operator outside Gibraltar to take any steps in a country or territory outside Gibraltar for the purpose of complying with a duty imposed by virtue of subsection (1) or (2) of that section, the matters to be taken into account include the following-

- (a) any requirements or restrictions under the law of that country or territory that are relevant to the taking of those steps; and
- (b) the extent to which it is reasonably practicable to comply with the duty in a way that does not breach any of those requirements or restrictions.

(4) Nothing in the definition of "telecommunications operator" limits the type of communications data in relation to which an authorisation, or a request or requirement of a kind which gives rise to a duty under section 58(1) or (2), may apply.

### **Part 3: interpretation.**

64.(1) In this Part-

"authorised officer" means a person in the service of or holding an office, rank or position with an intercepting authority;

"authorisation" means an authorisation for obtaining communications data granted under Part 3.

(2) See also-

section 2 (general definitions);

section 3 (telecommunications definitions);

section 4 (postal definitions).

(3) In this Part, "serious crime" means, in addition to crime which falls within paragraph (a) or (b) of the definition of "serious crime" in section 2, crime where the offence, or one of the offences, which is or would be constituted by the conduct concerned is-

- (a) an offence for which an individual who has reached the age of 18 is capable of being sentenced to imprisonment for a term of 12 months or more (disregarding any enactment prohibiting or restricting the imprisonment of individuals who have no previous convictions), or
- (b) an offence-
  - (i) by a person who is not an individual, or

- (ii) which involves, as an integral part of it, the sending of a communication or a breach of a person's privacy.

## **PART 4**

### **Equipment Interference**

#### *Authorisations under this Part*

#### **Authorisations under this Part: general.**

65.(1) A targeted equipment interference authorisation may be granted under this Part.

(2) A targeted equipment interference authorisation is an authorisation which authorises or requires the person to whom it is addressed to secure interference with any equipment for the purpose of obtaining-

- (a) communications (see section 88);
- (b) equipment data (see section 66);
- (c) any other information.

(3) A targeted equipment interference authorisation-

- (a) must also authorise or require the person to whom it is addressed to secure the obtaining of the communications, equipment data or other information to which the authorisation relates;
- (b) may also authorise that person to secure the disclosure, in any manner described in the authorisation, of anything obtained under the authorisation by virtue of paragraph (a).

(4) The reference in subsections (2) and (3) to the obtaining of communications or other information includes doing so by-

- (a) monitoring, observing or listening to a person's communications or other activities;
- (b) recording anything which is monitored, observed or listened to.

(5) A targeted equipment interference authorisation also authorises the following conduct (in addition to the conduct described in the authorisation)-

- (a) any conduct which it is necessary to undertake in order to do what is expressly authorised or required by the authorisation, including conduct for securing the obtaining of communications, equipment data or other information;

(b) any conduct by any person which is conduct in pursuance of a requirement imposed by or on behalf of the person to whom the authorisation is addressed to be provided with assistance in giving effect to the authorisation.

(6) A targeted equipment interference authorisation may not, by virtue of subsection (3), authorise or require a person to engage in conduct, in relation to a communication other than a stored communication, which would (unless done with lawful authority) constitute an offence under section 8(1) (unlawful interception).

(7) Subsection (5)(a) does not authorise a person to engage in conduct which could not be expressly authorised under the authorisation because of the restriction imposed by subsection (6).

(8) In subsection (6), "stored communication" means a communication stored in or by a telecommunication system (whether before or after its transmission).

(9) For provision enabling the combination of targeted equipment interference authorisations with certain other authorisations or notices see Schedule 3.

(10) Any conduct which is carried out in accordance with an authorisation under this Part is lawful for all purposes.

### **Meaning of "equipment data".**

66.(1) In this Part, "equipment data" means-

- (a) systems data;
- (b) data which falls within subsection (2).

(2) The data falling within this subsection is identifying data which-

- (a) is, for the purposes of a relevant system, comprised in, included as part of, attached to or logically associated with a communication (whether by the sender or otherwise) or any other item of information;
- (b) is capable of being logically separated from the remainder of the communication or the item of information; and
- (c) if it were so separated, would not reveal anything of what might reasonably be considered to be the meaning (if any) of the communication or the item of information, disregarding any meaning arising from the fact of the communication or the existence of the item of information or from any data relating to that fact.

(3) In subsection (2), "relevant system" means any system on or by means of which the data is held.

(4) For the meaning of "systems data" and "identifying data", see section 2.

**Subject-matter of authorisations.**

67. A targeted equipment interference authorisation may relate to any one or more of the following matters-

- (a) equipment belonging to, used by or in the possession of a particular person or organisation;
- (b) equipment belonging to, used by or in the possession of a group of persons who share a common purpose or who carry on, or may carry on, a particular activity;
- (c) equipment belonging to, used by or in the possession of more than one person or organisation, where the interference is for the purpose of a single investigation or operation;
- (d) equipment in a particular location;
- (e) equipment in more than one location, where the interference is for the purpose of a single investigation or operation;
- (f) equipment which is being, or may be, used for the purposes of a particular activity or activities of a particular description;
- (g) equipment which is being, or may be, used to test, maintain or develop capabilities relating to interference with equipment for the purpose of obtaining communications, equipment data or other information;
- (h) equipment which is being, or may be, used for the training of persons who carry out, or are likely to carry out, such interference with equipment.

*Power to grant authorisations*

**Power to grant targeted equipment interference authorisations.**

68.(1) The competent authority may, on an application made by an intercepting authority, grant a targeted equipment interference authorisation if the competent authority considers that-

- (a) the authorisation is necessary-
  - (i) for the purpose of preventing or detecting serious crime;
  - (ii) for the purpose of preventing death or any injury or damage to a person's physical or mental health or of mitigating any injury or damage to a person's physical or mental health;
  - (iii) in the interests of the security of Gibraltar; or

- (iv) in the interests of the economic well-being of Gibraltar so far as those interests are also relevant to the interest of the security of Gibraltar;
- (b) the conduct authorised by the authorisation is proportionate to what is sought to be achieved by that conduct; and
- (c) satisfactory arrangements made for the purposes of sections 82 and 83 (safeguards relating to disclosure etc.) are in force in relation to the authorisation.

(2) The competent authority on an application for a targeted equipment interference authorisation from an intercepting authority, who is the Principal Immigration Officer, may consider that the condition in subsection (1)(a) is satisfied only if the serious crime relates to an offence which is an immigration or nationality offence (whether or not it also relates to other offences).

(3) The competent authority on an application for a targeted equipment interference authorisation from an intercepting authority, who is the Collector of Customs, may consider that the condition in subsection (1)(a) is satisfied only if the serious crime relates to an assigned matter within the Imports and Exports Act, 1986.

(4) The competent authority must consider the matters referred to in subsection (1)(a) with a sufficient degree of care as to ensure that it complies with the duties imposed by section 7 (general duties in relation to privacy).

(5) Where the competent authority refuses to grant an authorisation under this Part, the competent authority must give written reasons for the refusal.

(6) Where the competent authority refuses to grant an authorisation under this Part, an intercepting authority may appeal the decision to the Supreme Court.

(7) For the purpose of subsection (2), an offence is an immigration or nationality offence if conduct constituting the offence-

- (a) relates to the entitlement of one or more persons who are not nationals of Gibraltar to enter, transit across, or be in, Gibraltar (including conduct which relates to conditions or other controls on any such entitlement); or
- (b) is undertaken for the purposes of or otherwise in relation to-
  - (i) the Immigration, Asylum and Refugee Act;
  - (ii) Borders & Coastguard Agency Act 2011;

**Restriction on grant of targeted equipment interference authorisations.**

69.(1) The competent authority may not grant a targeted equipment interference authorisation under section 68 unless it considers that there is a Gibraltar connection.

(2) For the purpose of this section, there is a Gibraltar connection if-

- (a) any of the conduct authorised by the authorisation would take place in Gibraltar (regardless of the location of the equipment that would, or may, be interfered with);
- (b) any of the equipment which would, or may, be interfered with would, or may, be in Gibraltar at some time while the interference is taking place; or
- (c) a purpose of the interference is to obtain-
  - (i) communications sent by, or to, a person who is, or whom an intercepting authority believes to be, for the time being in Gibraltar;
  - (ii) information relating to an individual who is, or whom an intercepting authority believes to be, for the time being in Gibraltar; or
  - (iii) equipment data which forms part of, or is connected with, communications or information falling within sub-paragraph (i) or (ii).

*Additional safeguards*

**Members of Parliament, etc.**

70. Schedule 5 applies where-

- (a) an application is made under section 68 to the competent authority by an intercepting authority for a targeted equipment interference authorisation; and
- (b) the purpose of the authorisation is to obtain-
  - (i) communications sent by, or intended for, a person who is a Member of Parliament; or
  - (ii) a Member of Parliament's private information.

**Items subject to legal privilege.**

71.(1) Subsections (2) to (5) apply if-

- (a) an application is made by an intercepting authority to the competent authority for an authorisation under this Part; and

- (b) the purpose, or one of the purposes, of the authorisation is to authorise or require interference with equipment for the purpose of obtaining items subject to legal privilege.

(2) The application must contain a statement that the purpose, or one of the purposes, of the authorisation is to authorise or require interference with equipment for the purpose of obtaining items subject to legal privilege.

(3) In deciding whether to grant the authorisation, the competent authority must have regard to the public interest in the confidentiality of items subject to legal privilege.

(4) The competent authority may grant the authorisation only if it considers-

- (a) that there are exceptional and compelling circumstances which make it necessary to authorise or require interference with equipment for the purpose of obtaining items subject to legal privilege; and
- (b) that the arrangements made for the purposes of section 82 include specific arrangements for the handling, retention, use and destruction of such items.

(5) The authorisation may not be issued if it is considered necessary only as mentioned in section 68(1)(a)(iv).

(6) For the purposes of subsection (4)(a), there cannot be exceptional and compelling circumstances that make it necessary to authorise or require interference with equipment for the purpose of obtaining items subject to legal privilege unless-

- (a) the public interest in obtaining the information that would be obtained by the authorisation outweighs the public interest in the confidentiality of items subject to legal privilege;
- (b) there are no other means by which the information may reasonably be obtained; and
- (c) obtaining the information in the case of an authorisation is considered necessary for the purposes of preventing or detecting serious crime or obtaining the information is necessary for the purpose of preventing death or significant injury.

(7) Subsections (8) and (9) apply if-

- (a) an application is made by an intercepting authority to the competent authority for an authorisation under this Part;
- (b) the applicant considers that the relevant material is likely to include items subject to legal privilege; and
- (c) subsections (2) to (5) do not apply.

(8) The application must contain-

- (a) a statement that the applicant considers that the relevant material is likely to include items subject to legal privilege; and
- (b) an assessment of how likely it is that the relevant material will include such items.

(9) The competent authority may grant the authorisation only if it considers that the arrangements made for the purposes of section 82 include specific arrangements for the handling, retention, use and destruction of items subject to legal privilege.

(10) In this section, "relevant material" means any material the obtaining of which is authorised or required under the authorisation.

(11) Subsections (12) and (13) apply if-

- (a) an application is made by an intercepting authority to the competent authority for an authorisation under this Part;
- (b) the purpose, or one of the purposes, of the authorisation is to authorise or require interference with equipment for the purpose of obtaining communications or other items of information that, if they were not communications made or (as the case may be) other items of information created or held with the intention of furthering a criminal purpose, would be items subject to legal privilege; and
- (c) the applicant considers that the communications or the other items of information ("the targeted communications or other items of information") are likely to be communications made or (as the case may be) other items of information created or held with the intention of furthering a criminal purpose.

(12) The application must-

- (a) contain a statement that the purpose, or one of the purposes, of the authorisation is to authorise or require interference with equipment for the purpose of obtaining communications or other items of information that, if they were not communications made or (as the case may be) other items of information created or held with the intention of furthering a criminal purpose, would be items subject to legal privilege; and
- (b) set out the reasons for believing that the targeted communications or other items of information are likely to be communications made or (as the case may be) other items of information created or held with the intention of furthering a criminal purpose.

(13) The competent authority may grant the authorisation only if it considers that the targeted communications or other items of information are likely to be communications made or (as

the case may be) other items of information created or held with the intention of furthering a criminal purpose.

**Confidential journalistic material.**

72.(1) This section applies if an application is made by an intercepting authority to the competent authority for an authorisation under this Part and the purpose, or one of the purposes, of the authorisation is to authorise or require interference with equipment for the purpose of obtaining communications or other items of information which the applicant for the authorisation believes will be communications or other items of information containing confidential journalistic material.

(2) The application must contain a statement that the purpose, or one of the purposes, of the authorisation is to authorise or require interference with equipment for the purpose of obtaining communications or other items of information which the applicant for the authorisation believes will be communications or other items of information containing confidential journalistic material.

(3) The competent authority may grant the authorisation only if it considers that the arrangements made for the purposes of section 82 include specific arrangements for the handling, retention, use and destruction of communications or other items of information containing confidential journalistic material.

(4) For the meaning of "journalistic material" and "confidential journalistic material", see section 5.

**Sources of journalistic information.**

73.(1) This section applies if an application is made by an intercepting authority to the competent authority for an authorisation under this Part and the purpose, or one of the purposes, of the authorisation is to identify or confirm a source of journalistic information.

(For the meaning of "source of journalistic information", see section 2(1).)

(2) The application must contain a statement that the purpose, or one of the purposes, of the authorisation is to identify or confirm a source of journalistic information.

(3) The competent authority may grant the authorisation only if it considers that the arrangements made for the purposes of section 82 include specific arrangements for the handling, retention, use and destruction of communications or other items of information that identify sources of journalistic information.

*Further provision about targeted equipment interference authorisations*

**Requirements that must be met by targeted equipment interference authorisations.**

74.(1) An authorisation under this Part must contain a provision stating it is a targeted equipment interference authorisation.

(2) An authorisation granted under section 68 must be addressed by the competent authority to an intercepting authority who made the application.

(3) In the case of a targeted equipment interference authorisation which relates to a matter described in the first column of the Table below, the authorisation must include the details specified in the second column.

<i>Matter</i>	<i>Details to be included in the authorisation</i>
Equipment belonging to, used by or in the possession of a particular person or organisation	The name of the person or organisation or a description of the person or organisation
Equipment belonging to, used by or in the possession of persons who form a group which shares a common purpose or who carry on, or may carry on, a particular activity	A description of the purpose or activity and the name of, or a description of, as many of the persons as it is reasonably practicable to name or describe
Equipment used by or in the possession of more than one person or organisation, where the interference is for the purpose of a single investigation or operation	A description of the nature of the investigation or operation and the name of, or a description of, as many of the persons or organisations as it is reasonably practicable to name or describe
Equipment in a particular location	A description of the location
Equipment in more than one location, where the interference is for the purpose of a single investigation or operation	A description of the nature of the investigation or operation and a description of as many of the locations as it is reasonably practicable to describe
Equipment which is being, or may be, used for the purposes of a particular activity or activities of a particular description	A description of the particular activity or activities
Equipment which is being, or may be, used to test, maintain or develop capabilities relating to interference with equipment	A description of the nature of the testing, maintenance or development of capabilities
Equipment which is being, or may be, used for the training of persons who carry out, or are likely to carry out, interference with equipment	A description of the nature of the training

(4) A targeted equipment interference authorisation must also describe-

- (a) the type of equipment which is to be interfered with; and
- (b) the conduct which the person to whom the authorisation is addressed is authorised to take.

**Duration of targeted equipment interference authorisations.**

75.(1) An authorisation granted under this Part ceases to have effect at the end of the relevant period (see subsection (2)), unless-

- (a) it is renewed before the end of that period (see section 76); or
- (b) it is cancelled or otherwise ceases to have effect before the end of that period (see section 78).

(2) In this section, "the relevant period" means the period of 6 months beginning with-

- (a) the day on which the authorisation was granted; or
- (b) in the case of an authorisation which has been renewed, the day after the day at the end of which the authorisation would have ceased to have effect if it had not been renewed.

**Renewal of targeted equipment interference authorisations.**

76.(1) If the renewal conditions are met, an authorisation granted under this Part may be renewed by the competent authority, at any time during the renewal period, on application made by an intercepting authority.

(2) The renewal conditions are that the competent authority considers that the-

- (a) authorisation continues to be necessary on any relevant grounds; and
- (b) conduct that would be authorised by the renewed authorisation continues to be proportionate to what is sought to be achieved by that conduct.

(3) In subsection (2)(a), "relevant grounds" means the purpose mentioned in section 68(1)(a)(i) to (iv).

(4) "The renewal period" means the period of 30 days ending with the day at the end of which the authorisation would otherwise cease to have effect.

(5) Section 68 applies in relation to a decision to renew an authorisation under this Part as it applies in relation to a decision to grant such an authorisation (and accordingly any reference in that section to the person who decided to grant the authorisation is to be read as a reference to the person who decided to renew it).

(6) Sections 70 to 73 (additional safeguards) apply in relation to a decision to renew an authorisation under this Part as they apply in relation to a decision to grant such an authorisation.

(7) In this section "relevant period" has the same meaning as in section 75.

**Modification of targeted equipment interference authorisations.**

77.(1) The provisions of an authorisation granted under section 68 may be modified at any time by the competent authority on application made by an intercepting authority.

(2) The only modifications which may be made under this section are-

- (a) adding to the matters to which the authorisation relates (see section 67, by including the details required in relation to that matter by section 74(3));
- (b) removing a matter to which the authorisation relates;
- (c) adding (in relation to a matter to which the authorisation relates) a name or description to the names or descriptions included in the authorisation in accordance with section 74(3);
- (d) varying or removing (in relation to a matter to which the authorisation relates) a name or description included in the authorisation in accordance with section 74(3);
- (e) adding to the descriptions of types of equipment included in the authorisation in accordance with section 74(4)(a);
- (f) varying or removing a description of a type of equipment included in the authorisation in accordance with section 74(4)(a).

(3) But where an authorisation relates only to a matter specified in section 67(a), only to a matter specified in section 67(d), or only to both such matters, the details included in the authorisation in accordance with section 74(3) may not be modified.

(4) A modification may be made only if (except in the case of a modification removing any matter, name or description), the competent authority considers that-

- (a) the modification is necessary on any relevant grounds (see subsection (5)); and
- (b) the conduct authorised by the modification is proportionate to what is sought to be achieved by that conduct.

(5) In subsection (4)(a), "relevant grounds" means the purpose mentioned in section 68(1)(a)(i) to (iv).

(6) Sections 70 to 73 (additional safeguards) apply in relation to the making of a modification to an authorisation under this section, other than a modification removing any matter, name or description, as they apply in relation to the issuing of an authorisation.

(7) In a case where any of sections 70 to 73 applies in relation to the making of a modification, section 68 applies in relation to a decision to make a modification of an authorisation as it applies in relation to a decision to grant such an authorisation, but as if the references in subsection (1)(a) and (b) of that section to the authorisation were references to the modification.

(8) Nothing in this section applies in relation to modifying the provisions of an authorisation in a way which does not affect the conduct authorised or required by it.

### **Cancellation of targeted equipment interference authorisations.**

78.(1) The competent authority may cancel an authorisation granted under this Part at any time on application made by an intercepting authority.

(2) If the competent authority considers that-

- (a) an authorisation granted under this Part is no longer necessary on any relevant grounds; or
- (b) the conduct authorised by an authorisation granted under this Part is no longer proportionate to what is sought to be achieved by the conduct,

it must cancel the authorisation.

(3) In subsection (2)(a), "relevant grounds" means the purpose mentioned in section 68(1)(a)(i) to (iv).

(4) Where an authorisation is cancelled under this section, the person to whom the authorisation was addressed must, so far as is reasonably practicable, secure that anything in the process of being done under the authorisation stops as soon as possible.

(5) An authorisation that has been cancelled under this section may not be renewed.

### *Implementation of authorisations*

### **Implementation of targeted equipment interference authorisations.**

79.(1) In giving effect to a targeted equipment interference authorisation, an intercepting authority may (in addition to acting alone) act through, or together with, such other persons as an intercepting authority may require (whether under subsection (2) or otherwise) to provide the authority with assistance in giving effect to the authorisation.

(2) For the purpose of requiring any person to provide assistance in relation to a targeted equipment interference authorisation, an intercepting authority may-

- (a) serve a copy of the authorisation on any person whom an intercepting authority considers may be able to provide such assistance; or
- (b) make arrangements for the service of a copy of the authorisation on any such person.

(3) A copy of an authorisation may be served under subsection (2) on a person outside Gibraltar for the purpose of requiring the person to provide such assistance in the form of conduct outside Gibraltar.

(4) For the purposes of this Act, the provision of assistance in giving effect to a targeted equipment interference authorisation includes any disclosure to an intercepting authority, or to persons acting on that person's behalf, of material obtained under the authorisation.

(5) The references in subsections (2) and (3) and sections 80 and 81 to the service of a copy of an authorisation include-

- (a) the service of a copy of one or more schedules contained in the authorisation with the omission of the remainder of the authorisation; and
- (b) the service of a copy of the authorisation with the omission of any schedule contained in it.

### **Service of authorisations.**

80.(1) This section applies to the service of authorisations under section 79(2).

(2) A copy of the authorisation must be served in such a way as to bring the contents of the authorisation to the attention of the person who an intercepting authority considers may be able to provide assistance in relation to it.

(3) A copy of an authorisation may be served on a person outside Gibraltar in any of the following ways (as well as by electronic or other means of service)-

- (a) by serving it at the person's principal office within Gibraltar or, if the person has no such office in Gibraltar, at any place in Gibraltar where the person carries on business or conducts activities;
- (b) if the person has specified an address in Gibraltar as one at which the person, or someone on the person's behalf, will accept service of documents of the same description as a copy of an authorisation, by serving it at that address;
- (c) by making it available for inspection (whether to the person or to someone acting on the person's behalf) at a place in Gibraltar (but this is subject to subsection (4)).

(4) A copy of an authorisation may be served on a person outside Gibraltar in the way mentioned in subsection (3)(c) only if-

- (a) it is not reasonably practicable for a copy to be served by any other means (whether as mentioned in subsection (3)(a) or (b) or otherwise); and
- (b) an intercepting authority takes such steps as it considers appropriate for the purpose of bringing the contents of the authorisation, and the availability of a copy for inspection, to the attention of the person.

(5) The steps mentioned in subsection (4)(b) must be taken as soon as reasonably practicable after the copy of the authorisation is made available for inspection.

#### **Duty of telecommunications operators to assist with implementation.**

81.(1) A telecommunications operator, that has been served with a copy of an authorisation granted under section 68 by the competent authority and addressed to an intercepting authority, must take all steps for giving effect to the authorisation which are notified to the telecommunications operator by an intercepting authority.

(2) The competent authority may grant a targeted equipment interference authorisation to a telecommunications operator if it considers that-

- (a) it is necessary for the telecommunications operator to be required to take the steps; and
- (b) the steps are proportionate to what is sought to be achieved by them.

(3) A telecommunications operator is not required to take any steps which it is not reasonably practicable for the telecommunications operator to take.

(4) The duty imposed by subsection (1) is enforceable against a person in Gibraltar by civil proceedings by the Attorney-General for an injunction or for any other appropriate relief.

#### *Supplementary provision*

#### **Safeguards relating to retention and disclosure of material.**

82.(1) The competent authority must ensure, in relation to every targeted equipment interference authorisation granted by it, that arrangements are in force for securing that the requirements of subsections (2) and (5) are met in relation to the material obtained under the authorisation.

This is subject to subsection (10).

(2) The requirements of this subsection are met in relation to the material obtained under an authorisation if each of the following is limited to the minimum that is necessary for the authorised purposes (see subsection (3))-

- (a) the number of persons to whom any of the material is disclosed or otherwise made available;
- (b) the extent to which any of the material is disclosed or otherwise made available;
- (c) the extent to which any of the material is copied;
- (d) the number of copies that are made.

(3) For the purposes of subsection (2), something is necessary for the authorised purposes if, and only if-

- (a) it is, or is likely to become, necessary on any relevant grounds (see subsection (7));
- (b) it is necessary for facilitating the carrying out of any functions under this Act by the person to whom the authorisation is or was addressed;
- (c) it is necessary for facilitating the carrying out of any functions of the competent authority under or in relation to this Act;
- (d) it is necessary for the purpose of legal proceedings; or
- (e) it is necessary for the performance of the functions of any person under any enactment.

(4) The arrangements for the time being in force under this section for securing that the requirements of subsection (2) are met in relation to the material obtained under the authorisation must include arrangements for securing that every copy made of any of that material is stored, for so long as it is retained, in a secure manner.

(5) The requirements of this subsection are met in relation to the material obtained under an authorisation if every copy made of any of that material (if not destroyed earlier) is destroyed as soon as there are no longer any grounds for retaining it (see subsection (6)).

(6) For the purposes of subsection (5), there are no longer any grounds for retaining a copy of any material if, and only if-

- (a) its retention is not necessary, or not likely to become necessary, on any relevant grounds (see subsection (7)); and
- (b) its retention is not necessary for any of the purposes mentioned in paragraphs (b) to (e) of subsection (3) above.

(7) In subsections (3) and (6), "relevant grounds" means the purpose mentioned in section 68(1)(a)(i) to (iv).

(8) Where-

- (a) material obtained under a targeted equipment interference authorisation is retained, following its examination, for purposes other than the destruction of the material; and
- (b) it is material that contains confidential journalistic material or identifies a source of journalistic material,

the person to whom the authorisation is addressed must inform the competent authority as soon as is reasonably practicable.

(9) Subsection (10) applies if-

- (a) any material obtained under the authorisation has been handed over to any overseas authorities; or
- (b) a copy of any such material has been given to any overseas authorities.

(10) To the extent that the requirements of subsections (2) and (5) relate to any of the material mentioned in subsection (9)(a), or to the copy mentioned in subsection (9)(b), the arrangements made for the purpose of this section are not required to secure that those requirements are met (see instead section 83).

(11) In this section-

"copy", in relation to material obtained under an authorisation, means any of the following (whether or not in documentary form)-

- (a) any copy, extract or summary of the material which identifies the material as having been obtained under the authorisation; and
- (b) any record which is a record of the identities of persons who owned, used or were in possession of the equipment which was interfered with to obtain that material,

and "copied" is to be read accordingly;

"overseas authorities" means authorities of a country or territory outside Gibraltar.

### **Safeguards relating to disclosure of material overseas.**

83.(1) The competent authority must ensure, in relation to every targeted equipment interference authorisation, that arrangements are in force for securing that-

- (a) any material obtained under the authorisation is handed over to overseas authorities only if the requirements of subsection (2) are met; and

- (b) copies of any such material are given to overseas authorities only if those requirements are met.

(2) The requirements of this subsection are met in the case of an authorisation if it appears to the competent authority that requirements corresponding to the requirements of section 82(2) and (5) will apply, to such extent (if any) as it considers appropriate, in relation to any of the material which is handed over, or any copy of which is given, to the authorities in question.

(3) In this section-

"copy" has the same meaning as in section 82;

"overseas authorities" means authorities of a country or territory outside Gibraltar.

**Additional safeguards for items subject to legal privilege.**

84.(1) This section applies where an item subject to legal privilege which has been obtained under a targeted equipment interference authorisation is retained, following its examination, for purposes other than the destruction of the item.

(2) The person to whom the authorisation is addressed must inform the competent authority of the retention of the item as soon as is reasonably practicable.

(3) Unless the competent authority considers that subsection (5) applies to the item, it must-

- (a) direct that the item is destroyed; or
- (b) impose one or more conditions as to the use or retention of that item.

(4) If the competent authority considers that subsection (5) applies to the item, it may nevertheless impose such conditions under subsection (3)(b) as it considers necessary for the purpose of protecting the public interest in the confidentiality of items subject to legal privilege.

(5) This subsection applies to an item subject to legal privilege if-

- (a) the public interest in retaining the item outweighs the public interest in the confidentiality of items subject to legal privilege; and
- (b) retaining the item is necessary in the interests of the security of Gibraltar or for the purpose of preventing death or significant injury.

(6) The competent authority-

- (a) may require an affected party to make representations about how it should exercise any function under subsection (3); and

- (b) must have regard to any such representations made by an affected party (whether or not as a result of a requirement imposed under paragraph (a)).

(7) For the purposes of subsection (6) the person to whom the authorisation is or was addressed is an “affected party”.

**Duty not to make unauthorised disclosures.**

85.(1) A person to whom this section applies must not make an unauthorised disclosure to another person.

- (2) A person makes an unauthorised disclosure for the purposes of this section if-
  - (a) the person discloses any of the matters within subsection (4) in relation to an authorisation under this Part; and
  - (b) the disclosure is not an excepted disclosure (see section 86).
- (3) This section applies to the following persons-
  - (a) any person who may apply for an authorisation under this Part;
  - (b) any person holding office under the Crown in right of the Government of Gibraltar;
  - (c) any person employed by, or for the purposes of, the Royal Gibraltar Police or HM Customs Gibraltar;
  - (d) any telecommunications operator;
  - (e) any person employed or engaged for the purposes of any business of a telecommunications operator;
  - (f) any person to whom any of the matters within subsection (4) have been disclosed in relation to an authorisation under this Part.
- (4) The matters referred to in subsection (2)(a) are-
  - (a) the existence or contents of the authorisation;
  - (b) the details of the grant of the authorisation or of any renewal or modification of the authorisation;
  - (c) the existence or contents of any requirement to provide assistance in giving effect to the authorisation;
  - (d) the steps taken in pursuance of the authorisation or of any such requirement;

- (e) any of the material obtained under the authorisation in a form which identifies it as having been obtained under an authorisation under this Part.

**Section 85: meaning of "excepted disclosure".**

86.(1) For the purposes of section 85, a disclosure made in relation to an authorisation is an excepted disclosure if it falls within any of the Heads set out in-

- (a) subsection (2) (disclosures authorised by authorisation etc.);
- (b) subsection (3) (oversight bodies);
- (c) subsection (4) (legal proceedings);
- (d) subsection (6) (disclosures of a general nature).

(2) Head 1 is-

- (a) a disclosure authorised by the authorisation;
- (b) a disclosure authorised by the person to whom the authorisation is or was addressed or under any arrangements made by that person for the purposes of this section;
- (c) a disclosure authorised by the terms of any requirement to provide assistance in giving effect to the authorisation (including any requirement for disclosure imposed by virtue of section 79(4)).

(3) Head 2 is a disclosure made to, or authorised by, the competent authority;

(4) Head 3 is-

- (a) a disclosure made-
  - (i) in contemplation of, or in connection with, any legal proceedings; and
  - (ii) for the purposes of those proceedings;
- (b) a disclosure made-
  - (i) by a professional legal adviser ("L") to L's client or a representative of L's client; or
  - (ii) by L's client, or by a representative of L's client, to L,

in connection with the giving, by L to L's client, of advice about the effect of the provisions of this Part.

(5) But a disclosure within Head 3 is not an excepted disclosure if it is made with the intention of furthering a criminal purpose.

(6) Head 4 is-

(a) a disclosure which-

- (i) is made by a telecommunications operator in accordance with a requirement imposed by regulations made by the Minister; and
- (ii) consists of statistical information of a description specified in the regulations;

(b) a disclosure of information that does not relate to any particular authorisation under this Part but relates to such authorisations in general.

#### **Offence of making unauthorised disclosure.**

87.(1) A person commits an offence if-

- (a) the person discloses any matter in breach of section 85(1); and
- (b) the person knew that the disclosure was in breach of that section.

(2) A person who is guilty of an offence under this section is liable-

(a) on summary conviction in Gibraltar-

- (i) to imprisonment for a term not exceeding 12 months; or
- (ii) to a fine,

or to both;

(b) on conviction on indictment, to imprisonment for a term not exceeding 5 years or to a fine, or to both.

(3) In proceedings against any person for an offence under this section in respect of any disclosure, it is a defence for the person to show that the person could not reasonably have been expected, after first becoming aware of the matter disclosed, to take steps to prevent the disclosure.

#### **Part 4: interpretation.**

88.(1) In this Part-

"communication" includes-

- (a) anything comprising speech, music, sounds, visual images or data of any description; and
- (b) signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus;

"equipment" means equipment producing electromagnetic, acoustic or other emissions or any device capable of being used in connection with such equipment;

"equipment data" has the meaning given by section 66;

"private information" includes information relating to a person's private or family life;

(2) See also-

section 2 (general definitions);

section 3 (telecommunications definitions);

section 5 (general definitions: "journalistic material" etc.).

## **PART 5**

### **Surveillance and Covert Investigations and entry on or interference with property and radiocommunication**

#### **Chapter 1**

##### **Directed surveillance, Intrusive surveillance and Covert Human Intelligence Sources**

###### *Introductory*

###### **Conduct to which Chapter 1 applies.**

89.(1) This Chapter applies to the following conduct-

- (a) directed surveillance;
- (b) intrusive surveillance;
- (c) the conduct and use of covert human intelligence sources; and
- (d) criminal conduct in the course of, or otherwise in connection with, the conduct of covert human intelligence sources.

(2) Subject to subsection (7), surveillance is directed for the purposes of this Chapter if it is covert but not intrusive and is undertaken-

- (a) for the purposes of a specific investigation or a 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 authorisation under this Chapter to be sought for the carrying out of the surveillance.

(3) Subject to subsections (4) to (7), surveillance is intrusive for the purposes of this Chapter if, and only if, it is 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.

(4) For the purposes of this Chapter surveillance is not intrusive to the extent that-

- (a) it is carried out by means only of a surveillance device designed or adapted principally for the purpose of providing information about the location of a vehicle; or
- (b) it is surveillance consisting in any such interception of a communication as falls within section 107(4).

(5) For the purposes of this Chapter surveillance which-

- (a) is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle, but
- (b) is carried out without that device being present on the premises or in the vehicle,

is not intrusive unless the device is such that it 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.

(6) For the purposes of this Chapter surveillance which-

- (a) is carried out by means of apparatus designed or adapted for the purpose of detecting the installation or use in any residential or other premises of a television receiver; and

(b) is carried out from outside those premises exclusively for that purpose,

is neither directed nor intrusive.

(7) For the purposes of this Chapter directed surveillance that is carried out in relation to anything taking place on so much of any premises specified in subsection (8) as is, at any time during the surveillance, used for the purpose of legal consultations shall be treated as intrusive surveillance.

(8) The following premises are specified for the purposes of subsection (7)-

- (a) any place in which persons who are serving sentences of imprisonment or detention, remanded in custody or committed in custody for trial or sentence may be detained;
- (b) any place in which persons may be detained under the Immigration, Asylum and Refugee Act;
- (c) any place in which persons may be detained under the Criminal Procedure and Evidence Act 2011;
- (d) any place in which persons may be detained under the Imports and Exports Act, 1986;
- (e) police stations;
- (f) the place of business of any professional legal adviser; and
- (g) any place used for the sittings and business of any court or inquest or inquiry.

(9) In this Part-

- (a) references to the conduct of a covert human intelligence source are references to any conduct of such a source which falls within any of paragraphs (a) to (c) of subsection (10), or is incidental to anything falling within any of those paragraphs; and
- (b) references to the use of a covert human intelligence source are references to inducing, asking or assisting a person to engage in the conduct of such a source, or to obtain information by means of the conduct of such a source.

(10) For the purposes of this Chapter a person is a covert human intelligence source if-

- (a) he 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 covertly uses such a relationship to obtain information or to provide access to any information to another person; or
- (c) he covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

(11) In this Chapter references to criminal conduct in the course of, or otherwise in connection with, the conduct of a covert human intelligence source are references to any conduct that-

- (a) disregarding this Part, would constitute crime; and
- (b) consists of, is in the course of, or is otherwise in connection with, the conduct of a covert human intelligence source.

(12) For the purposes of this section-

- (a) surveillance is covert if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place;
- (b) 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; and
- (c) a relationship is used covertly, and information obtained as mentioned in subsection (10)(c) 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.

(13) In this section "private information", in relation to a person, includes any information relating to his private or family life.

(14) References in this section, in relation to a vehicle, to the presence of a surveillance device in the vehicle include references to its being located on or under the vehicle and also include references to its being attached to it.

*Authorisations for directed surveillance, intrusive surveillance and human intelligence sources*

**Lawful surveillance etc.**

90.(1) Conduct to which this Chapter applies shall be lawful for all purposes if-

- (a) an authorisation under this Chapter confers an entitlement to engage in that conduct on the person whose conduct it is; and

(b) his conduct is in accordance with the authorisation.

(2) A person shall not be subject to any civil liability in respect of any conduct of his which-

(a) is incidental to any conduct that is lawful by virtue of subsection (1); and

(b) is not itself conduct an authorisation is capable of being granted under this Act and might reasonably have been expected to have been sought in the case in question.

(3) The conduct that may be authorised under this Chapter includes conduct outside Gibraltar.

#### **Authorisations for directed surveillance.**

91.(1) Subject to the following provisions of this Part, an intercepting authority shall have power for the purposes of this section to grant authorisations for the carrying out of directed surveillance.

(2) An intercepting authority shall not grant an authorisation for the carrying out of directed surveillance unless it believes that the-

(a) authorisation is necessary on grounds falling within subsection (3); and

(b) authorised surveillance is proportionate to what is sought to be achieved by carrying it out.

(3) An authorisation is necessary on grounds falling within this subsection if it is necessary-

(a) in the interests of the security of Gibraltar;

(b) for the purpose of preventing or detecting crime or of preventing disorder;

(c) in the interests of the economic well-being of Gibraltar;

(d) in the interests of public safety;

(e) for the purposes of protecting public health; or

(f) for the purposes of assessing or collecting any tax, duty, levy or other imposition, contribution of charge payable to a government department.

(4) The matters to be taken into account in considering whether the requirements of subsection (2) are satisfied in the case of any authorisation shall include whether the information which it is thought necessary to obtain by the authorised conduct could reasonably be obtained by other means.

(5) The conduct that is authorised by an authorisation for the carrying out of directed surveillance is any conduct that-

- (a) consists in the carrying out of directed surveillance of any such description as is specified in the authorisation; and
- (b) is carried out in the circumstances described in the authorisation and for the purposes of the investigation or operation specified or described in the authorisation.

**Authorisations for intrusive surveillance.**

92.(1) Subject to the following provisions of this Part, the competent authority shall have power for the purposes of this section to grant authorisations on application by an intercepting authority for the carrying out of intrusive surveillance.

(2) The competent authority shall not grant an authorisation for the carrying out of intrusive surveillance unless it believes that the-

- (a) authorisation is necessary on grounds falling within subsection (3); and
- (b) authorised surveillance is proportionate to what is sought to be achieved by carrying it out.

(3) Subject to the following provisions of this section, an authorisation is necessary on grounds falling within this subsection if it is necessary-

- (a) in the interests of the security of Gibraltar;
- (b) for the purpose of preventing or detecting serious crime; or
- (c) in the interests of the economic well-being of Gibraltar.

(4) The matters to be taken into account in considering whether the requirements of subsection (2) are satisfied in the case of any authorisation shall include whether the information which it is thought necessary to obtain by the authorised conduct could reasonably be obtained by other means.

(5) The conduct that is authorised by an authorisation for the carrying out of intrusive surveillance is any conduct that-

- (a) consists in the carrying out of intrusive surveillance of any such description as is specified in the authorisation;
- (b) is carried out in relation to the residential premises specified or described in the authorisation or in relation to the private vehicle so specified or described; and

- (c) is carried out for the purposes of, or in connection with, the investigation or operation so specified or described.

**Authorisations for covert human intelligence sources.**

93.(1) Subject to the following provisions of this Part-

- (a) the competent authority shall have power for the purposes of this section to grant authorisations on application by an intercepting authority for the conduct or the use of a covert human intelligence source involving a juvenile source or a vulnerable adult source; and
- (b) an intercepting authority shall have power for the purposes of this section to grant authorisations for a standard covert human intelligence source.

(2) The competent authority or an intercepting authority shall not grant an authorisation for the conduct or the use of a covert human intelligence source (involving a juvenile source or a vulnerable adult source) or a standard covert human intelligence source, as applicable, unless it believes-

- (a) that the authorisation is necessary on grounds falling within subsection (3);
- (b) that the authorised conduct or use is proportionate to what is sought to be achieved by that conduct or use; and
- (c) that arrangements exist for the source's case that satisfy the requirements of subsection (6) and such other requirements as may be prescribed by regulations made by the Minister.

(3) An authorisation is necessary on grounds falling within this subsection if it is necessary-

- (a) in the interests of the security of Gibraltar;
- (b) for the purpose of preventing or detecting crime or of preventing disorder;
- (c) in the interests of the economic well-being of Gibraltar;
- (d) in the interests of public safety;
- (e) for the purposes of protecting public health; or
- (f) for the purposes of assessing or collecting any tax, duty, levy or other imposition, contribution of charge payable to a government department.

(4) The matters to be taken into account in considering whether the requirements of subsection (2) are satisfied in the case of any authorisation shall include whether the

information which it is thought necessary to obtain by the authorised conduct could reasonably be obtained by other means.

(5) The conduct that is authorised by an authorisation for the conduct or the use of a covert human intelligence source (involving a juvenile source or a vulnerable adult source) or a standard covert human intelligence source is any conduct that-

- (a) is comprised in any such activities involving conduct of a source, or the use of a source, as are specified or described in the authorisation;
- (b) consists in conduct by or in relation to the person who is so specified or described as the person to whose actions as a source the authorisation relates; and
- (c) is carried out for the purposes of, or in connection with, the investigation or operation so specified or described.

(6) For the purposes of this Chapter there are arrangements for the source's case that satisfy the requirements of this subsection if such arrangements are in force as are necessary for ensuring that-

- (a) there will at all times be a person holding an office, rank or position with the intercepting authority who will have day-to-day responsibility for dealing with the source on behalf of that authority, and for the source's security and welfare;
- (b) there will at all times be another person holding an office, rank or position with the intercepting authority who will have general oversight of the use made of the source;
- (c) there will at all times be a person holding an office, rank or position with the intercepting authority who will have responsibility for maintaining a record of the use made of the source;
- (d) the records relating to the source that are maintained by the intercepting authority will always contain particulars of all such matters (if any) as may be specified for the purposes of this paragraph in regulations made by the Minister; and
- (e) records maintained by the intercepting authority that disclose the identity of the source will not be available to persons except to the extent that there is a need for access to them to be made available to those persons.

*Sources under 16: prohibition (section 93)*

(7) No authorisation under section 93 may be granted for the conduct or use of a source if-

- (a) the source is under the age of sixteen; and

- (b) the relationship to which the conduct or use would relate is between the source and his parent or any parent who has parental responsibility for him.

*Sources under 16: arrangements for meetings (section 93)*

(8) For the purposes of section 93-

- (a) where the source is under the age of sixteen, the arrangements referred to in subsection (2)(c) shall be such that there is at all times a person holding an office, rank or position with the intercepting authority who has responsibility for ensuring that an appropriate adult is present at meetings to which this subsection applies.
- (b) subsection 8(a) applies to all meetings between the source and a person representing any intercepting authority that take place while the source remains under the age of sixteen.
- (c) in paragraph (a), “appropriate adult” means-
  - (i) the parent or guardian of the source;
  - (ii) any other person who has for the time being assumed responsibility for his welfare or is otherwise qualified to represent the interests of the source; or
  - (iii) where no person falling within paragraph (i) or (ii) is available, any responsible person aged eighteen or over who is neither a member of nor employed by any intercepting authority.

*Sources under 18: risk assessments etc. (section 93)*

(9) An authorisation under section 93 for the conduct or use of a source may not be granted or renewed in any case where the source is under the age of eighteen at the time of the grant or renewal, unless-

- (a) a person holding an office, rank or position with the intercepting authority has made and, in the case of a renewal, updated a risk assessment sufficient to demonstrate that-
  - (i) the nature and magnitude of any risk of physical injury to the source arising in the course of, or as a result of, carrying out the conduct described in the authorisation have been identified and evaluated; and
  - (ii) the nature and magnitude of any risk of psychological distress to the source arising in the course of, or as a result of, carrying out the conduct described in the authorisation have been identified and evaluated;
- (b) the competent authority issuing or renewing the authorisation has considered the risk assessment and has satisfied itself that any risks identified in it are justified

and, if they are, that they have been properly explained to and understood by the source; and

- (c) the competent authority issuing or renewing the authorisation knows whether the relationship to which the conduct or use would relate is between the source and a relative, guardian or person who has for the time being assumed responsibility for the source's welfare, and, if it is, has given particular consideration to whether the authorisation is justified in the light of that fact.

*Sources under 18: duration of authorisations (section 93)*

(10) In relation to an authorisation under section 93 for the conduct or the use of a source who is under the age of eighteen at the time the authorisation is granted or renewed, section 99(3) shall have effect as if the period specified in paragraph (a) of that subsection were one month instead of twelve months.

(11) An authorisation for the conduct or the use of a covert human intelligence source does not authorise any criminal conduct in the course of, or otherwise in connection with, the conduct of a covert human intelligence source (but see section 94 for provision for the authorisation of such conduct).

(12) An authorisation under this section may not have the effect of authorising a covert human intelligence source who is a person designated under section 74 of the Police Act 2006 to establish contact in person with another person.

(13) The Minister may by order-

- (a) prohibit the authorisation under this section of any such conduct or uses of sources as may be described in the order; and
- (b) impose requirements, in addition to those provided for by subsection (2), that must be satisfied before an authorisation is granted under this section for any such conduct or uses of sources as may be so described.

(14) In the case of any authorisation for the conduct or the use of a source whose activities are to be for the benefit of more than one intercepting authority, the references in subsection (6) to the intercepting authority are references to one of them (whether or not the same one in the case of each reference).

(15) In this section "source" means a covert human intelligence source and includes a juvenile source and a vulnerable adult source as applicable.

**Covert human intelligence sources: criminal conduct authorisations.**

94.(1) Subject to the following provisions of this Part-

- (a) the competent authority shall have power for the purposes of this section to grant criminal conduct authorisations involving a juvenile source or a vulnerable adult source on application by an intercepting authority; and
- (b) an intercepting authority shall have power for the purposes of this section to grant standard criminal conduct authorisations.

(2) A “criminal conduct authorisation” is an authorisation for criminal conduct in the course of, or otherwise in connection with, the conduct of a covert human intelligence source.

(3) A criminal conduct authorisation (involving a juvenile source or a vulnerable adult source) or standard criminal conduct authorisation may only be granted in relation to a covert human intelligence source after, or at the same time as, an authorisation under section 93 which authorises the conduct or the use of the covert human intelligence source concerned.

(4) The competent authority or an intercepting authority may not grant a criminal conduct authorisation (involving a juvenile source or a vulnerable adult source) or a standard criminal conduct authorisation, as applicable, unless it believes-

- (a) that the authorisation is necessary on grounds falling within subsection (5);
- (b) that the authorised conduct is proportionate to what is sought to be achieved by that conduct; and
- (c) that arrangements exist that satisfy such requirements as may be imposed by order made by the Minister.

(5) An authorisation is necessary on grounds falling within this subsection if it is necessary-

- (a) in the interests of security of Gibraltar;
- (b) for the purpose of preventing or detecting crime or of preventing disorder; or
- (c) in the interests of the economic well-being of Gibraltar.

(6) The matters to be taken into account in considering whether the requirements in subsection (4)(a) and (b) are satisfied, shall include whether what is sought to be achieved by the authorised conduct could reasonably be achieved by other conduct which would not constitute crime.

(7) Subsection (6) is without prejudice to the need to take into account other matters so far as they are relevant (for example, the requirements of the Gibraltar Constitution Order 2006).

(8) The conduct that is authorised by a criminal conduct authorisation (involving a juvenile source or a vulnerable adult source) or standard criminal conduct authorisation, as applicable, is any conduct that-

- (a) is comprised in any activities-
  - (i) which involve criminal conduct in the course of, or otherwise in connection with, the conduct of a covert human intelligence source, and
  - (ii) are specified or described in the authorisation;
- (b) consists in conduct by or in relation to the person who is so specified or described as the covert human intelligence source to whom the authorisation relates; and
- (c) is carried out for the purposes of, or in connection with, the investigation or operation so specified or described.

(9) If an authorisation under section 93, which authorises the conduct or the use of a covert human intelligence source (involving a juvenile source or a vulnerable adult source) or standard covert human intelligence source, to whom a criminal conduct authorisation relates, ceases to have effect, the criminal conduct authorisation (involving a juvenile source or a vulnerable adult source) or standard criminal conduct authorisation, as applicable, also ceases to have effect so far as it relates to that covert human intelligence source, (but this is without prejudice to whether the criminal conduct authorisation (involving a juvenile source or a vulnerable adult source) or standard criminal conduct authorisations continues to have effect so far as it relates to any other covert human intelligence source).

(10) The Minister may by order-

- (a) prohibit the authorisation under this section of any such conduct as may be described in the order; and
- (b) impose requirements, in addition to those provided for by subsections (3) and (4) and sections 95 and 96, that must be satisfied before an authorisation is granted under this section for any such conduct as may be so described.

### **Criminal conduct authorisations: safeguards for juveniles.**

95.(1) This section applies in relation to the grant of a juvenile criminal conduct authorisation granted by the competent authority.

(2) “A juvenile criminal conduct authorisation” is an authorisation under section 94 for criminal conduct in the course of, or otherwise in connection with, the conduct of a covert human intelligence source where that source is under the age of 18 (“the juvenile source”).

(3) In addition to satisfying the requirements of section 94, the competent authority may grant a juvenile criminal conduct authorisation only if-

- (a) the competent authority has considered the results of an appropriate risk assessment;

- (b) there are exceptional circumstances such that-
    - (i) it is not reasonably foreseeable in the circumstances as the competent authority believes them to be that any harm to the juvenile source would result from the grant of the authorisation, and
    - (ii) the competent authority believes the authorisation would be compatible with the need to safeguard and promote the best interests of the juvenile source; and
  - (c) the competent authority believes that appropriate arrangements for meetings are in force.
- (4) For the purposes of subsection (3)(a), “an appropriate risk assessment” means an assessment which-
- (a) identifies and evaluates the nature and magnitude of the risks of harm to the juvenile source arising in the course of, or as result of, the conduct authorised by the authorisation; and
  - (b) is carried out in accordance with provision made by the Minister by regulations under this paragraph.
- (5) In subsections (3)(b)(i) and (4)(a), “harm” means-
- (a) physical injury; or
  - (b) psychological distress.
- (6) For the purposes of subsection (3)(c), “appropriate arrangements for meetings” are such arrangements for the juvenile source's case as are necessary for ensuring-
- (a) that, at all times when the juvenile source is under the age of 16, there will be a relevant person who will have responsibility for ensuring that an appropriate adult is present at all meetings in relation to the authorisation which take place between the source and a person representing an intercepting authority; and
  - (b) that, at all times when the juvenile source is 16 or 17 years old, there will be a relevant person within an intercepting authority who will have responsibility for-
    - (i) ensuring that an appropriate adult is present at all meetings in relation to the authorisation which take place between the source and a person representing an intercepting authority, other than any such meeting in relation to which a relevant person decides there are circumstances which justify the absence of an appropriate adult, and

- (ii) maintaining a record of the reasons for each such decision that there are circumstances in relation to a meeting which justify the absence of an appropriate adult.

(7) In subsection (6)-

“appropriate adult”, in relation to a juvenile source, means-

- (a) the parent or guardian of the juvenile source; or
- (b) any other person who-
  - (i) has for the time being assumed responsibility for the juvenile source's welfare, or
  - (ii) is otherwise qualified to represent the interests of the juvenile source;

“intercepting authority”, in relation to a juvenile criminal conduct authorisation, refers to an intercepting authority defined in section 2 of this Act, for whose benefit the activities of the juvenile source as a covert human intelligence source are to take place;

“relevant person”, in relation to a juvenile criminal conduct authorisation, means a person holding an office, rank or position within an intercepting authority in relation to the authorisation.

*Sources under 16: prohibition (section 94)*

(8) No authorisation under section 94 may be granted authorising criminal conduct in the course of, or otherwise in connection with, the conduct of a source if-

- (a) the source is under the age of 16; and
- (b) the relationship to which the relevant conduct would relate is between the source and-
  - (i) the source's parent, or
  - (ii) any person who has parental responsibility for the source.

*Sources under 18: additional requirements (section 94)*

(9) An authorisation under section 94 may not be granted or renewed in any case where the source to whom the authorisation relates is under the age of 18 at the time of the grant or renewal unless the intercepting authority granting or renewing the authorisation-

- (a) has considered whether the relationship to which the relevant conduct would relate is between the source and-
  - (i) a relative or guardian of the source, or
  - (ii) a person who has for the time being assumed responsibility for the source's welfare; and
- (b) where the relationship would so relate, has taken that fact into account as a particular consideration.

*Sources under 18: arrangements regarding best interests of the source (section 94)*

(10) Where the source to whom an authorisation under section 94 relates is under the age of 18, the arrangements referred to in section 94(4)(c) must be such that there is at all times a relevant person who has responsibility for safeguarding and promoting the best interests of the source.

*Sources under 18: duration of authorisations (section 94)*

(11) In relation to an authorisation under section 94 where the source to whom the authorisation relates is under the age of 18 at the time the authorisation is granted or renewed, section 99(3) is to have effect as if the period specified in paragraph (a) of that subsection were four months instead of twelve months.

(12) For the purposes of this section-

“relevant conduct” means the conduct of the source which the authorised conduct would be in the course of or otherwise in connection with;

“relevant person”, in relation to a juvenile criminal conduct authorisation, means a person holding an office, rank or position within an intercepting authority in relation to the authorisation;

“source” means a covert human intelligence source.

(13) No provision made by or under this section affects the power to make additional provision by order under section 94(4)(c) or (10) in relation to the grant of a juvenile criminal conduct authorisation.

**Criminal conduct authorisations: safeguards for vulnerable adults.**

96.(1) This section applies in relation to the grant of a vulnerable adult criminal conduct authorisation by the competent authority.

(2) “A vulnerable adult criminal conduct authorisation” is an authorisation under section 94 for criminal conduct in the course of, or otherwise in connection with, the conduct of a covert

human intelligence source where that source is a vulnerable adult (“the vulnerable adult source”).

(3) For the purposes of this section, a “vulnerable adult” is a person aged 18 or over who by reason of mental disorder or vulnerability, disability, age or illness, is or may be unable to take care of themselves or to protect themselves against significant harm or exploitation.

(4) In addition to satisfying the requirements of section 94, the competent authority may grant a vulnerable adult criminal conduct authorisation only if it-

- (a) has considered the results of an appropriate risk assessment;
- (b) believes that the risks of harm identified by that risk assessment have been properly explained to and understood by the vulnerable adult source; and
- (c) has taken into account the need to safeguard and promote the best interests of the vulnerable adult source.

(5) “An appropriate risk assessment” means an assessment which-

- (a) identifies and evaluates the nature and magnitude of the risks of harm to the vulnerable adult source arising in the course of, or as result of, the conduct authorised by the authorisation; and
- (b) is carried out in accordance with provision made by the Minister by regulations under this paragraph.

(6) For the purposes of subsections (3), (4)(b) and (5)(a), “harm” means-

- (a) physical injury; or
- (b) psychological distress.

(7) No provision made by or under this section affects the power to make additional provision by order under section 94(4)(c) or (10) in relation to the grant of a vulnerable adult criminal conduct authorisation.

**Procedure for authorisations: directed surveillance, standard covert human intelligence sources and standard criminal conduct authorisations.**

97.(1) Subject to the following provisions of this Part, an intercepting authority shall have power to grant authorisations for-

- (a) directed surveillance,
- (b) standard covert human intelligence sources;

- (c) standard criminal conduct authorisations.
- (2) An intercepting authority is not required to give notice of the application to-
- (a) any person to whom the authorisation relates, or
  - (b) such a person's legal representatives.
- (3) The authorisation shall not take effect until it has been granted by an intercepting authority in accordance with subsection (4).
- (4) An intercepting authority may grant the authorisation if, and only if, it-
- (a) is satisfied that there are reasonable grounds for believing that the requirements of-
    - (i) section 91(2) in relation to directed surveillance;
    - (ii) section 93(2) in relation to standard covert human intelligence sources, or
    - (iii) section 94(4) in relation to standard criminal conduct authorisations,are satisfied in the case of the authorisation;
  - (b) shall, as soon as reasonably practicable after making that decision, grant an authorisation and give notice of its decision.
- (5) Where an intercepting authority grants or cancels a standard criminal conduct authorisation under this section, it must give notice to the competent authority.
- (6) A notice given for the purposes of (5) must be given-
- (a) in writing as soon as practicable and, in any event, before the end of the period of 7 days beginning with the day after that on which the authorisation to which it relates is granted or cancelled; and
  - (b) in accordance with such arrangements made for the purposes of this paragraph by the competent authority as are for the time being in force.
- (7) A notice under this section relating to the grant of an authorisation under section 94 must-
- (a) set out the grounds on which the intercepting authority giving the notice believes that the requirements of section 94(4) are satisfied in relation to the authorisation; and
  - (b) specify the conduct that is authorised under section 94 by the authorisation.

(8) Any notice that is required by this section to be given in writing may be given instead, by being transmitted by electronic means.

**Procedure for authorisations: intrusive surveillance, covert human intelligence sources involving a juvenile source or a vulnerable adult source and criminal conduct authorisations involving a juvenile source or a vulnerable adult source.**

98.(1) An intercepting authority shall apply to the competent authority for an authorisation for-

- (a) intrusive surveillance,
- (b) covert human intelligence sources involving a juvenile source or a vulnerable adult source;
- (c) criminal conduct authorisations involving a juvenile source or a vulnerable adult source.

(2) An intercepting authority is not required to give notice of the application to-

- (a) any person to whom the authorisation relates, or
- (b) such a person's legal representatives.

(3) The authorisation shall not take effect until it has been granted by the competent authority in accordance with subsection (4), to the intercepting authority who applied for the authorisation.

(4) The competent authority may grant the authorisation if, and only if, it-

- (a) is satisfied that there are reasonable grounds for believing that the requirements of-
  - (i) section 92(2) in relation to intrusive surveillance;
  - (ii) section 93(2) in relation to covert human intelligence sources involving a juvenile source or a vulnerable adult source, or
  - (iii) section 94(4) in relation to criminal conduct authorisations involving a juvenile source or a vulnerable adult source,

are satisfied in the case of the authorisation; and

- (b) shall, as soon as reasonably practicable after making that decision, grant an authorisation and give notice of its decision to the intercepting authority who applied for the authorisation.

(5) If the competent authority decides not to grant an authorisation to which subsection (3) applies, it shall reject the application and make a report of its findings to the intercepting authority who applied for the authorisation.

(6) The intercepting authority may appeal to the Supreme Court against the decision made by the competent authority under subsection (5).

(7) On an appeal under subsection (6), the Supreme Court may-

- (a) confirm the competent authority's decision; or
- (b) make a fresh determination.

*Grant, renewal and duration of authorisations*

**General rules about grant, renewal and duration.**

99.(1) An authorisation under this Chapter shall be granted or renewed in writing by the competent authority or an intercepting authority, as applicable.

(2) A single authorisation may combine two or more different authorisations under this Part; but the provisions of this Act that are applicable in the case of each of the authorisations shall apply separately in relation to the part of the combined authorisation to which they are applicable.

(3) Subject to sections 93(10) and 95(11) in relation to juvenile covert human intelligence sources and subsections (4) and (8) below, an authorisation under this Chapter shall cease to have effect at the end of the following period-

- (a) in a case in which the authorisation is for the conduct or the use of a covert human intelligence source or criminal conduct authorisation under section 94, the period of twelve months beginning with the day on which the grant of the authorisation or, as the case may be, its latest renewal takes effect; and
- (b) in any case not falling within paragraph (a), the period of three months beginning with the day on which the grant of the authorisation or, as the case may be, its latest renewal takes effect.

(4) Subject to subsection (6), an authorisation under this Chapter may be renewed on the same terms, at any time before the time at which it ceases to have effect, by the competent authority or an intercepting authority who granted the authorisation.

(5) Sections 91 to 97 shall have effect in relation to the renewal of an authorisation under this Chapter as if references to the grant of an authorisation included references to its renewal.

(6) The competent authority or an intercepting authority, as applicable, shall not renew an authorisation for the conduct or the use of a covert human intelligence source (to include conduct or the use of a standard covert human intelligence source) or an authorisation under section 94 (to include standard criminal conduct authorisations) unless it -

- (a) is satisfied that a review has been carried out of the matters mentioned in subsection (7) below, and
- (b) has, for the purpose of deciding whether to renew the authorisation, considered the results of that review.

(7) The matters mentioned in subsection (6) are-

- (a) the use made of the source in the period since the grant or, as the case may be, latest renewal of the authorisation; and
- (b) the tasks given to the source during that period and the information obtained from the conduct or the use of the source.

(8) The competent authority or an intercepting authority, as applicable, may provide in relation to authorisations of such descriptions that subsection (3) is to have effect as if the period at the end of which an authorisation of a description so specified is to cease to have effect were such period shorter than that provided for by that subsection as may be fixed by or determined in accordance with that authorisation.

(9) References in this section to the time at which, or the day on which, the grant or renewal of an authorisation takes effect are references-

- (a) in the case of the grant of an authorisation, to the time at which or, as the case may be, day on which the authorisation is granted; and
- (b) in the case of the renewal of an authorisation, to the time at which or, as the case may be, day on which the authorisation would have ceased to have effect but for the renewal.

(10) For the purposes of this section “in writing” includes electronic means.

(11) For the purposes of the grant of an authorisation that combines-

- (a) an authorisation under section 91, 93(1)(b) or 94(1)(b), and
- (b) an authorisation by the competent authority for the carrying out of intrusive surveillance under section 92,

the competent authority shall be granting the authorisation for the purposes of that section.

**Cancellation of authorisations by the competent authority.**

100.(1) The competent authority who granted or renewed an authorisation under this Chapter may cancel it on application by an intercepting authority if-

- (a) it is satisfied that the authorisation is one in relation to which the requirements of section 92(2)(a) and (b), 93(2)(a) and (b) or, as the case may be, 94(4)(a) and (b) are no longer satisfied;
- (b) in the case of an authorisation under section 93, it is satisfied that arrangements for the source's case that satisfy the requirements mentioned in subsection (2)(c) of that section no longer exist;
- (c) in the case of an authorisation under section 94 where the source is under the age of 18 (“the juvenile source”), the competent authority-
  - (i) becomes aware of circumstances in which it is reasonably foreseeable that harm, within the meaning of section 95(5), to the juvenile source would result from the authorisation,
  - (ii) is satisfied that the authorisation would no longer be compatible with the need to safeguard and promote the best interests of the juvenile source, or
  - (iii) is satisfied that arrangements for the juvenile source's case that satisfy the requirements of subsection (3)(c) of section 95 no longer exist; or
- (d) in the case of any authorisation under section 94, the competent authority is satisfied that any arrangements for the source's case required to satisfy any requirements mentioned in subsection (4)(c) of that section no longer exist.

(2) An application from an intercepting authority to the competent authority for cancellation of an authorisation must contain the following matters-

- (a) the reasons for seeking cancellation of the authorisation;
- (b) the outcome of the investigation to which the authorisations related, and details of any criminal proceedings instituted or intended to be instituted; and
- (c) what arrangements have been made for the storage of material obtained as a result of the conduct authorised, for its review and its destruction when its retention is no longer required, and for the immediate destruction of any material unrelated to the purposes for which the conduct was authorised.

(3) When the competent authority cancels an authorisation it must notify the intercepting authority who made the application of the date and time when conduct, previously authorised, is to cease.

**Cancellation of authorisations by an intercepting authority.**

101.(1) Subject to the provisions in section 97(5) to (8) in relation to standard criminal conduct authorisations, an intercepting authority, who granted or renewed an authorisation under this Chapter may cancel it if-

- (a) it is satisfied that the authorisation is one in relation to which the requirements of section 91(2)(a) and (b), 93(2)(a) and (b) or, as the case may be, 94(4)(a) and (b) are no longer satisfied;
- (b) in the case of an authorisation under section 93, it is satisfied that arrangements for the source's case that satisfy the requirements mentioned in subsection (2)(c) of that section no longer exist;
- (c) in the case of any authorisation under section 94, an intercepting authority is satisfied that any arrangements for the source's case required to satisfy any requirements mentioned in subsection (4)(c) of that section no longer exist.

(2) An application to an intercepting authority for cancellation of an authorisation must contain the following matters-

- (a) the reasons for seeking cancellation of the authorisation;
- (b) the outcome of the investigation to which the authorisations related, and details of any criminal proceedings instituted or intended to be instituted; and
- (c) what arrangements have been made for the storage of material obtained as a result of the conduct authorised, for its review and its destruction when its retention is no longer required, and for the immediate destruction of any material unrelated to the purposes for which the conduct was authorised.

(3) When an intercepting authority cancels an authorisation, it must make a note of the date and time when conduct, previously authorised, is to cease.

**Chapter 2**

**Authorisations in respect of entry on or interference with property or radiocommunication**

**Entry on or interference with property or radiocommunication.**

102. No entry on or interference with property or with radiocommunication shall be unlawful if it is authorised by an authorisation granted by the competent authority on application by an intercepting authority under this Chapter.

**Authorisations to enter on or interfere with property or radiocommunication.**

103.(1) Where subsection (2) applies, the competent authority may grant an authorisation to authorise-

- (a) the taking of such action in respect of such property as it may specify; or
- (b) the taking of such action as it may specify, in respect of radiocommunication.

(2) This subsection applies where the competent authority believes that-

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

(3) The matters to be taken into account in considering whether the requirements of subsection (2) are satisfied in the case of any authorisation shall include whether what it is thought necessary to achieve by the authorisation could reasonably be achieved by other means.

(4) The competent authority shall not grant an authorisation under this section except upon an application by an intercepting authority.

(5) The powers conferred by this section are additional to any other powers which a person has by virtue of any other enactment and are not to be taken to affect any of those other powers.

**Authorisations: form and duration.**

104.(1) An authorisation under this Chapter shall be in writing and for the purposes of this section this includes electronic means.

(2) An authorisation shall, unless renewed under subsection (3) cease to have effect at the end of the period of three months beginning with the day on which it took effect.

(3) If at any time before an authorisation would cease to have effect the competent authority, on application by an intercepting authority, considers it necessary for the authorisation to continue to have effect for the purpose for which it was granted, it may in writing renew it for a period of three months beginning with the day on which it would cease to have effect.

(4) The competent authority shall cancel any authorisation if satisfied that the authorisation is one in relation to which the requirements of section 103(2)(a) and (b) are no longer satisfied.

### **Chapter 3**

#### **Supplemental provision for Part 5**

##### **Power to extend or modify authorisations.**

105. An intercepting authority who wishes to extend or modify an authorisation, after it has been granted under this Part, is required to make a new application to the competent authority.

##### **Matters subject to legal privilege: covert human intelligence sources.**

106.(1) This section applies where any conduct that is, or is to be, authorised by an authorisation under section 93 consists of activities involving conduct of a source, or the use of a source, to-

- (a) obtain matters subject to legal privilege;
- (b) provide access to any matters subject to legal privilege to another person; or
- (c) disclose matters subject to legal privilege.

(2) Subject to subsection (3), an authorisation for such conduct shall not be granted or renewed unless it satisfies the requirements imposed by this section.

(3) Where a single authorisation under section 93 authorises conduct to which this section applies and other conduct falling within this Act, the requirements imposed by this section shall only apply in relation to those parts of the combined authorisation which authorise conduct falling within subsection (1).

(4) Where an intercepting authority makes an application to the competent authority seeking an authorisation under this section, it has to provide the competent authority with notice in writing specifying-

- (a) the grounds on which it believes the matters specified in subsection 8 and section 93(2)(b) and (c);
- (b) the conduct falling within subsection 1 that is, or is to be, authorised by the authorisation;
- (c) the identity, where known, of the-
  - (i) legal representative and his client or any person representing his client; or
  - (ii) legal representative or his client or any such representative and any other person,

to whom the activities of the source relates;

- (d) the matters subject to legal privilege (to the extent known) to which the conduct that is to be authorised by the authorisation relate; and
- (e) whether the conduct to be authorised is likely to result in the obtaining of private information about any person who is not specifically identified in the notice for the purposes of the investigation or operation.

(5) Where an intercepting authority makes an application to the competent authority seeking a renewal of an authorisation under this section, it has to provide the competent authority with notice in writing specifying-

- (a) whether the authorisation is being renewed for the first time, or, where it has been previously renewed, each occasion on which it has been renewed;
- (b) the matters required by subsection (4), as they apply at the time of the notice seeking approval to renew;
- (c) every aspect (if any) in which the information contained in the previous notice under this section has changed;
- (d) the reason why it is considered necessary to renew the authorisation;
- (e) the content and value to the investigation or operation of the matters subject to legal privilege obtained from the conduct or the use of the source in the period since the grant of the authorisation;
- (f) the results of any reviews of the matters mentioned in section 99(7); and
- (g) the period for which the authorisation is considered likely to continue to be necessary.

(6) Where the competent authority receives an application under this section, it must as soon as reasonably practicable-

- (a) scrutinise the application with the accompanying notice; and
- (b) decide whether or not to approve the grant or renewal of the authorisation.

(7) The competent authority shall-

- (a) give his approval to the grant or renewal of the authorisation if, and only if, it is satisfied that there are reasonable grounds for believing that-
  - (i) the authorisation is necessary on grounds falling within subsection 8; and

- (ii) the requirements of section 93(2)(b) and (c) or as the case may be section 94(4)(b) and (c) are satisfied in the case of the authorisation; and
  - (b) give written notice of his decision to the person who made the application as soon as reasonably practicable after making that decision.
- (8) An authorisation is necessary on the grounds falling within this section if it is necessary-
- (a) in the interests of the security of Gibraltar;
  - (b) for the purpose of preventing or detecting serious crime; or
  - (c) in the interests of the economic well-being of Gibraltar.
- (9) Any notice required by this section to be given in writing may be given instead by electronic means.
- (10) The duration of an authorisation granted under this section shall be three months.

### **Interpretation of Part 5.**

107.(1) In this Part-

"covert human intelligence source" shall be construed in accordance with section 89(10);

"directed" and "intrusive", in relation to surveillance, shall be construed in accordance with section 89(2) to (8);

"private vehicle" means (subject to subsection (6)(a)) 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;

"residential premises" means (subject to subsection (6)(b)) so much of any premises as is for the time being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation (including hotel or prison accommodation that is so occupied or used);

"surveillance" shall be construed in accordance with subsections (2) to (4);

"surveillance device" means any apparatus designed or adapted for use in surveillance.

(2) Subject to subsection (3), in this Part "surveillance" includes-

- (a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications;

(b) recording anything monitored, observed or listened to in the course of surveillance;  
and

(c) surveillance by or with the assistance of a surveillance device.

(3) References in this Part to surveillance do not include references to-

(a) any conduct of a covert human intelligence source for obtaining or recording (whether or not using a surveillance device) any information which is disclosed in the presence of the source;

(b) the use of a covert human intelligence source for so obtaining or recording information; or

(c) any such entry on or interference with property or with radiocommunication as would be unlawful, unless authorised under Part 4 (equipment interference) or Chapter 2 of Part 5 (interference with property or radiocommunication) of this Act.

(4) References in this Part to surveillance include references to the interception of a communication in the course of its transmission by means of a postal service or communication system if, and only if-

(a) the communication is one sent by or intended for a person who has consented to the interception of communications sent by or to him; and

(b) there is no interception authorisation authorising the interception.

(5) For the purposes of this Part the activities of a covert human intelligence source which are to be taken as activities for the benefit of a particular intercepting authority include any conduct of his as such a source which is in response to inducements or requests made by that authority.

(6) In subsection (1)-

(a) the reference to a person having the right to use a vehicle does not, in relation to a motor vehicle, include a reference to a person whose right to use the vehicle derives only from his having paid, or undertaken to pay, for the use of the vehicle and its driver for a particular journey; and

(b) the reference to premises occupied or used by any person for residential purposes or otherwise as living accommodation does not include a reference to so much of any premises as constitutes any common area to which he has or is allowed access in connection with his use or occupation of any accommodation.

(7) In this section-

"premises" includes any vehicle or moveable structure and any other place whatever, whether or not occupied as land;

"vehicle" includes any vessel, aircraft or hovercraft.

## **PART 6**

### **Investigation of Electronic Data Protected by Encryption etc.**

#### *Power to require disclosure*

#### **Notices requiring disclosure (“Disclosure notices”).**

108.(1) This section applies where any protected information-

- (a) has come into the possession of any person by means of the exercise of a statutory power to seize, detain, inspect, search or otherwise to interfere with documents or other property, or is likely to do so;
- (b) has come into the possession of any person by means of the exercise of any statutory power to intercept communications or obtain secondary data from communications in accordance with section 20, or is likely to do so;
- (c) has come into the possession of any person by means of the exercise of any power conferred by an authorisation under Part 3, Part 4 or Part 5 of this Act, or is likely to do so;
- (d) has come into the possession of any person as a result of having been provided or disclosed in pursuance of any statutory duty (whether or not one arising as a result of a request for information), or is likely to do so; or
- (e) has, by any other lawful means not involving the exercise of statutory powers, come into the possession of an intercepting authority, or is likely so to come into the possession of an intercepting authority.

(2) If the competent authority, on application made by an intercepting authority, believes on reasonable grounds-

- (a) that a key to the protected information is in the possession of any person;
- (b) that the imposition of a disclosure requirement in respect of the protected information is-
  - (i) necessary on grounds falling within subsection (3); or

- (ii) necessary for the purpose of securing the effective exercise or proper performance by any public authority of any statutory power or statutory duty;
- (c) that the imposition of such a requirement is proportionate to what is sought to be achieved by its imposition; and
- (d) that it is not reasonably practicable for an intercepting authority with the appropriate permission to obtain possession of the protected information in an intelligible form without the giving of a notice under this section,

it may grant a notice (a “disclosure notice”) to the person whom it believes to have possession of the key, imposing a disclosure requirement in respect of the protected information.

(3) A disclosure requirement in respect of any protected information is necessary on grounds falling within this subsection if it is necessary-

- (a) in the interests of the security of Gibraltar;
- (b) for the purpose of preventing or detecting crime; or
- (c) in the interests of the economic well-being of Gibraltar.

(4) A notice under this section imposing a disclosure requirement in respect of any protected information shall-

- (a) be given in writing or (if not in writing) shall be given in a manner that produces a record of its having been given;
- (b) describe the protected information to which the notice relates;
- (c) specify the matters falling within subsection (2)(b)(i) or (ii) by reference to which the notice is given;
- (d) specify the time by which the notice is to be complied with; and
- (e) set out the disclosure that is required by the notice and the form and manner in which it is to be made;

and the time specified for the purposes of paragraph (d) shall allow a period for compliance which is reasonable in all the circumstances.

(5) Where it appears to the competent authority-

- (a) that more than one person is in possession of the key to any protected information,

- (b) that any of those persons is in possession of that key in his capacity as an officer or employee of any body corporate, and
- (c) that another of those persons is the body corporate itself or another officer or employee of the body corporate,

a notice under this section shall not be granted, by reference to his possession of the key, to any officer or employee of the body corporate unless he is a senior officer of the body corporate or it appears to the competent authority issuing the notice that there is no senior officer of the body corporate and (in the case of an employee) no more senior employee of the body corporate to whom it is reasonably practicable to give the notice.

(6) Where it appears to the competent authority-

- (a) that more than one person is in possession of the key to any protected information,
- (b) that any of those persons is in possession of that key in his capacity as an employee of a firm, and
- (c) that another of those persons is the firm itself or a partner of the firm,

a notice under this section shall not be granted, by reference to his possession of the key, to any employee of the firm unless it appears to the competent authority issuing the notice that there is neither a partner of the firm nor a more senior employee of the firm to whom it is reasonably practicable to grant the notice.

(7) Subsections (5) and (6) shall not apply to the extent that there are special circumstances of the case that mean that the purposes for which the notice is granted would be defeated, in whole or in part, if the notice were granted to the person to whom it would otherwise be required to be granted by those subsections.

(8) A notice under this section shall not require the making of any disclosure to any person other than-

- (a) the competent authority issuing the notice; or
- (b) such other person as may be specified in or otherwise identified by, or in accordance with, the provisions of the notice.

(9) A notice under this section shall not require the disclosure of any key which-

- (a) is intended to be used for the purpose only of generating electronic signatures; and
- (b) has not in fact been used for any other purpose.

(10) In this section "senior officer", in relation to a body corporate, means a director, manager, secretary or other similar officer of the body corporate; and for this purpose

"director", in relation to a body corporate whose affairs are managed by its members, means a member of the body corporate.

**Effect of notice imposing disclosure requirement.**

109.(1) Subject to the following provisions of this section, the effect of a disclosure notice imposing a disclosure requirement in respect of any protected information on a person who is in possession at a relevant time of both the protected information and a means of obtaining access to the information and of disclosing it in an intelligible form is that he-

- (a) shall be entitled to use any key in his possession to obtain access to the information or to put it into an intelligible form; and
- (b) shall be required, in accordance with the notice imposing the requirement, to make a disclosure of the information in an intelligible form.

(2) A person subject to a requirement under subsection (1)(b) to make a disclosure of any information in an intelligible form shall be taken to have complied with that requirement if-

- (a) he makes, instead, a disclosure of any key to the protected information that is in his possession; and
- (b) that disclosure is made, in accordance with the notice imposing the requirement, to the person to whom, and by the time by which, he was required to provide the information in that form.

(3) Where, in a case in which a disclosure requirement in respect of any protected information is imposed on any person by a disclosure notice-

- (a) that person is not in possession of the information;
- (b) that person is incapable, without the use of a key that is not in his possession, of obtaining access to the information and of disclosing it in an intelligible form; or
- (c) the notice states, in pursuance of a direction under section 110, that it can be complied with only by the disclosure of a key to the information,

the effect of imposing that disclosure requirement on that person is that he shall be required, in accordance with the notice imposing the requirement, to make a disclosure of any key to the protected information that is in his possession at a relevant time.

(4) Subsections (5) to (7) apply where a person ("the person given notice")-

- (a) is entitled or obliged to disclose a key to protected information for the purpose of complying with any disclosure requirement imposed by a disclosure notice; and
- (b) is in possession of more than one key to that information.

(5) It shall not be necessary, for the purpose of complying with the requirement, for the person given notice to make a disclosure of any keys in addition to those the disclosure of which is, alone, sufficient to enable the person to whom they are disclosed to obtain access to the information and to put it into an intelligible form.

(6) Where-

- (a) subsection (5) allows the person given notice to comply with a requirement without disclosing all of the keys in his possession, and
- (b) there are different keys, or combinations of keys, in the possession of that person the disclosure of which would, under that subsection, constitute compliance,

the person given notice may select which of the keys, or combination of keys, to disclose for the purpose of complying with that requirement in accordance with that subsection.

(7) Subject to subsections (5) and (6), the person given notice shall not be taken to have complied with the disclosure requirement by the disclosure of a key unless he has disclosed every key to the protected information that is in his possession at a relevant time.

(8) Where, in a case in which a disclosure requirement in respect of any protected information is imposed on any person by a disclosure notice-

- (a) that person has been in possession of the key to that information but is no longer in possession of it,
- (b) if he had continued to have the key in his possession, he would have been required by virtue of the giving of the notice to disclose it, and
- (c) he is in possession, at a relevant time, of information to which subsection (9) applies,

the effect of imposing that disclosure requirement on that person is that he shall be required, in accordance with the notice imposing the requirement, to disclose all such information to which subsection (9) applies as is in his possession and as he may be required, in accordance with that notice, to disclose by the person to whom he would have been required to disclose the key.

(9) This subsection applies to any information that would facilitate the obtaining or discovery of the key or the putting of the protected information into an intelligible form.

(10) In this section "relevant time", in relation to a disclosure requirement imposed by a disclosure notice, means the time of the giving of the notice or any subsequent time before the time by which the requirement falls to be complied with.

**Cases in which key required.**

110.(1) A disclosure notice imposing a disclosure requirement in respect of any protected information shall not contain a statement for the purposes of section 109(3)(c) unless the competent authority who granted the notice in relation to that information, has given a direction that the requirement can be complied with only by the disclosure of the key itself.

(2) The competent authority shall not give a direction for the purposes of subsection (1) unless it believes-

- (a) that there are special circumstances of the case which mean that the purposes for which it was believed necessary to impose the requirement in question would be defeated, in whole or in part, if the direction were not given; and
- (b) that the giving of the direction is proportionate to what is sought to be achieved by prohibiting any compliance with the requirement in question otherwise than by the disclosure of the key itself.

(3) The matters to be taken into account in considering whether the requirement of subsection (2)(b) is satisfied in the case of any direction shall include-

- (a) the extent and nature of any protected information, in addition to the protected information in respect of which the disclosure requirement is imposed, to which the key is also a key; and
- (b) any adverse effect that the giving of the direction might have on a business carried on by the person on whom the disclosure requirement is imposed.

*Contributions to costs*

**Arrangements for payments for disclosure.**

111. It shall be the duty of the Minister with responsibility for Finance to ensure that such arrangements are in force as he thinks appropriate for requiring or authorising, in such cases as he thinks fit, the making to persons to whom disclosure notices are given of appropriate contributions towards the costs incurred by them in complying with such notices.

*Offences*

**Failure to comply with a notice.**

112.(1) A person to whom a disclosure notice has been given is guilty of an offence if he knowingly fails, in accordance with the notice, to make the disclosure required by virtue of the giving of the notice.

(2) In proceedings against any person for an offence under this section, if it is shown that that person was in possession of a key to any protected information at any time before the time

of the giving of the disclosure notice, that person shall be taken for the purposes of those proceedings to have continued to be in possession of that key at all subsequent times, unless it is shown that the key was not in his possession after the giving of the notice and before the time by which he was required to disclose it.

(3) For the purposes of this section a person shall be taken to have shown that he was not in possession of a key to protected information at a particular time if-

- (a) sufficient evidence of that fact is adduced to raise an issue with respect to it; and
- (b) the contrary is not proved beyond a reasonable doubt.

(4) In proceedings against any person for an offence under this section it shall be a defence for that person to show-

- (a) that it was not reasonably practicable for him to make the disclosure required by virtue of the giving of the disclosure notice before the time by which he was required, in accordance with that notice, to make it; but
- (b) that he did make that disclosure as soon after that time as it was reasonably practicable for him to do so.

(5) A person guilty of an offence under this section shall be liable-

- (a) on conviction on indictment, to imprisonment for a term not exceeding the appropriate maximum term or to a fine, or to both;
- (b) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum, or to both.

(6) In subsection (5) "the appropriate maximum term" means-

- (a) in a security of Gibraltar case or a child indecency case, five years; and
- (b) in any other case, two years.

(7) In subsection (6) "a security of Gibraltar case" means a case in which the grounds specified in the notice to which the offence relates as the grounds for imposing a disclosure requirement were or included a belief that the imposition of the requirement was necessary in the interests of the security of Gibraltar.

(8) In subsection (6) "a child indecency case" means a case in which the grounds specified in the notice to which the offence relates as the grounds for imposing a disclosure requirement were or included a belief that the imposition of the requirement was necessary for the purpose of preventing or detecting an offence under any of the provisions listed in subsection (9).

(9) Those provisions are-

- (a) section 257 of the Crimes Act 2011 (taking and publishing indecent photographs of children);
- (b) section 256 of the Crimes Act 2011 (simple possession of indecent photograph of a child);

**Tipping-off.**

113.(1) This section applies where a disclosure notice contains a provision requiring-

- (a) the person to whom the notice is given, and
- (b) every other person who becomes aware of it or of its contents,

to keep secret the giving of the notice, its contents and the things done in pursuance of it.

(2) A requirement to keep anything secret shall not be included in a disclosure notice except where it is included with the consent of the competent authority who granted the notice.

(3) A disclosure notice shall not contain a requirement to keep anything secret except where the protected information to which it relates-

- (a) has come into the possession of an intercepting authority, or
- (b) is likely to come into the possession of an intercepting authority,

by means which it is reasonable, in order to maintain the effectiveness of any investigation or operation or of investigatory techniques generally, or in the interests of the safety or well-being of any person, to keep secret from a particular person.

(4) A person who makes a disclosure to any other person of anything that he is required by a disclosure notice to keep secret shall be guilty of an offence and liable-

- (a) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine, or to both;
- (b) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum, or to both.

(5) In proceedings against any person for an offence under this section in respect of any disclosure, it shall be a defence for that person to show that-

- (a) the disclosure was effected entirely by the operation of software designed to indicate when a key to protected information has ceased to be secure; and

- (b) that person could not reasonably have been expected to take steps, after being given the notice or (as the case may be) becoming aware of it or of its contents, to prevent the disclosure.

(6) In proceedings against any person for an offence under this section in respect of any disclosure, it shall be a defence for that person to show that-

- (a) the disclosure was made by or to a professional legal adviser in connection with the giving, by the adviser to any client of his, of advice about the effect of provisions of this Part; and
- (b) the person to whom or, as the case may be, by whom it was made was the client or a representative of the client.

(7) In proceedings against any person for an offence under this section in respect of any disclosure, it shall be a defence for that person to show that the disclosure was made by a legal adviser-

- (a) in contemplation of, or in connection with, any legal proceedings; and
- (b) for the purposes of those proceedings.

(8) Neither subsection (6) nor subsection (7) applies in the case of a disclosure made with a view to furthering any criminal purpose.

(9) In proceedings against any person for an offence under this section in respect of any disclosure, it shall be a defence for that person to show that the disclosure was confined to a disclosure made or authorised-

- (a) by the terms of the notice;
- (b) by the person who gave the notice; or
- (c) by a person who-
  - (i) is in lawful possession of the protected information to which the notice relates; and
  - (ii) came into possession of that information as mentioned in section 108(1).

(10) In proceedings for an offence under this section against a person other than the person to whom the notice was given, it shall be a defence for the person against whom the proceedings are brought to show that he neither knew nor had reasonable grounds for suspecting that the notice contained a requirement to keep secret what was disclosed.

*Safeguards*

**General duties of specified authorities.**

114.(1) This section applies to-

- (a) an intercepting authority; and
- (b) every person whose officers or employees include persons with duties that involve the giving of disclosure notices.

(2) It shall be the duty of each of the persons to whom this section applies to ensure that such arrangements are in force, in relation to persons under his control who by virtue of this Part obtain possession of keys to protected information, as he considers necessary for securing-

- (a) that a key disclosed in pursuance of a disclosure notice is used for obtaining access to, or putting into an intelligible form, only protected information in relation to which power to give such a notice was exercised or could have been exercised if the key had not already been disclosed;
- (b) that the uses to which a key so disclosed is put are reasonable having regard both to the uses to which the person using the key is entitled to put any protected information to which it relates and to the other circumstances of the case;
- (c) that, having regard to those matters, the use and any retention of the key are proportionate to what is sought to be achieved by its use or retention;
- (d) that the requirements of subsection (3) are satisfied in relation to any key disclosed in pursuance of a disclosure notice;
- (e) that, for the purpose of ensuring that those requirements are satisfied, any key so disclosed is stored, for so long as it is retained, in a secure manner;
- (f) that all records of a key so disclosed (if not destroyed earlier) are destroyed as soon as the key is no longer needed for the purpose of enabling protected information to be put into an intelligible form.

(3) The requirements of this subsection are satisfied in relation to any key disclosed in pursuance of a disclosure notice if-

- (a) the number of persons to whom the key is disclosed or otherwise made available, and
- (b) the number of copies made of the key,

are each limited to the minimum that is necessary for the purpose of enabling protected information to be put into an intelligible form.

(4) Subject to subsection (5), where any relevant person incurs any loss or damage in consequence of-

- (a) any breach by a person to whom this section applies of the duty imposed on him by subsection (2), or
- (b) any contravention by any person whatever of arrangements made in pursuance of that subsection in relation to persons under the control of a person to whom this section applies,

the breach or contravention shall be actionable against the person to whom this section applies at the suit or instance of the relevant person.

(5) A person is a relevant person for the purposes of subsection (4) if he is-

- (a) a person who has made a disclosure in pursuance of a disclosure notice; or
- (b) a person whose protected information or key has been disclosed in pursuance of such a notice;

and loss or damage shall be taken into account for the purposes of that subsection to the extent only that it relates to the disclosure of particular protected information or a particular key which, in the case of a person falling with paragraph (b), shall be his information or key.

(6) For the purposes of subsection (5)-

- (a) information belongs to a person if he has any right that would be infringed by an unauthorised disclosure of the information; and
- (b) a key belongs to a person if it is a key to information that belongs to him or he has any right that would be infringed by an unauthorised disclosure of the key.

(7) In any proceedings brought by virtue of subsection (4), it shall be the duty of the court to have regard to any opinion with respect to the matters to which the proceedings relate that is or has been given by the competent authority or the Investigatory Powers Commissioner.

#### *Interpretation of Part 6*

#### **Interpretation of Part 6.**

115.(1) In this Part-

"electronic signature" means anything in electronic form which-

- (a) is incorporated into, or otherwise logically associated with, any electronic communication or other electronic data;

- (b) is generated by the signatory or other source of the communication or data; and
- (c) is used for the purpose of facilitating, by means of a link between the signatory or other source and the communication or data, the establishment of the authenticity of the communication or data, the establishment of its integrity, or both;

"key", in relation to any electronic data, means any key, code, password, algorithm or other data the use of which (with or without other keys)-

- (a) allows access to the electronic data, or
- (b) facilitates the putting of the data into an intelligible form;

"protected information" means any electronic data which, without the key to the data-

- (a) cannot, or cannot readily, be accessed, or
- (b) cannot, or cannot readily, be put into an intelligible form;

"disclosure notice" means a disclosure notice under section 108;

(2) References in this Part to a person's having information (including a key to protected information) in his possession include references-

- (a) to its being in the possession of a person who is under his control so far as that information is concerned;
- (b) to his having an immediate right of access to it, or an immediate right to have it transmitted or otherwise supplied to him; and
- (c) to its being, or being contained in, anything which he or a person under his control is entitled, in exercise of any statutory power and without otherwise taking possession of it, to detain, inspect or search.

(3) References in this Part to something's being intelligible or being put into an intelligible form include references to its being in the condition in which it was before an encryption or similar process was applied to it or, as the case may be, to its being restored to that condition.

(4) In this section-

- (a) references to the authenticity of any communication or data are references to any one or more of the following-
  - (i) whether the communication or data comes from a particular person or other source;

- (ii) whether it is accurately timed and dated;
  - (iii) whether it is intended to have legal effect; and
- (b) references to the integrity of any communication or data are references to whether there has been any tampering with or other modification of the communication or data.

## **PART 7**

### **Oversight Arrangements**

#### **Chapter 1**

##### **Investigatory Powers Commissioner**

###### *The Investigatory Powers Commissioner*

###### **Investigatory Powers Commissioner.**

116.(1) The Governor must appoint an Investigatory Powers Commissioner, in consultation with the Chief Minister, acting on the advice of the Judicial Services Commission.

(2) A person is not to be appointed as Investigatory Powers Commissioner unless-

- (a) the person holds or has held a high judicial office; or
- (b) is among persons recommended by-
  - (i) the Chief Minister; or
  - (ii) the Governor.

(3) The Investigatory Powers Commissioner may, to such extent as necessary, with approval from the Governor, delegate his functions in writing to such person as is suitably qualified and only where he-

- (a) is away from the jurisdiction; or
- (b) cannot, during a period of time, discharge the functions of his office due to illness or other inability.

(4) The delegation under subsection (3) to any extent of functions by the Investigatory Powers Commissioner does not prevent the exercise of the functions to that extent by that Commissioner.

**Terms and conditions of appointment.**

117.(1) Subject as follows, the Investigatory Powers Commissioner holds and vacates office in accordance with the Commissioner's terms and conditions of appointment.

(2) The Investigatory Powers Commissioner is to be appointed for a term of three years.

(3) A person who ceases to be the Investigatory Powers Commissioner (otherwise than under subsection (5)) may be re-appointed under section 116(1).

(4) The Investigatory Powers Commissioner may not, subject to subsection (5), be removed from office before the end of the term for which the Commissioner is appointed.

(5) The Investigatory Powers Commissioner may be removed from office by the Governor, acting with the agreement of the Chief Minister, for inability to discharge the functions of his office (whether arising from infirmity of body or mind or any other cause) or for misbehaviour.

*Main functions of the Investigatory Powers Commissioner*

**Main oversight functions.**

118.(1) The Investigatory Powers Commissioner must keep under review (including by way of audit, inspection and investigation) the exercise by a public authority of statutory functions authorised under this Act relating to-

- (a) the interception of communications;
- (b) the acquisition of communications data;
- (c) the acquisition of secondary data or related systems data under Chapter 1 of Part 2;
- (d) equipment interference;
- (e) surveillance, covert investigations, criminal conduct authorisations and entry and interference with property and radiocommunications under Part 5; and
- (f) investigation of electronic data protected by encryption under Part 6.

(2) Such statutory functions include, in particular, functions relating to the disclosure, retention or other use of-

- (a) any content of communications intercepted by an interception authorised or required by an authorisation under Chapter 1 of Part 2;
- (b) acquired communications data;

- (c) data acquired as mentioned in subsection (1)(c); or
- (d) communications, equipment data or other information acquired by means of equipment interference.

(3) But the Investigatory Powers Commissioner is not to keep under review-

- (a) the exercise of any function of a relevant Minister to make subsidiary legislation;
- (b) the exercise of any function by a judicial authority;
- (c) the exercise of any function which-
  - (i) is for the purpose of obtaining information or taking possession of any document or other property in connection with communications stored in or by a telecommunication system; or
  - (ii) is carried out in accordance with an order made by a judicial authority for that purpose,

and is not exercisable by virtue of this Act; or

- (d) the exercise of any function where the conduct concerned is-
  - (i) conduct authorised by section 40 or 42; or
  - (ii) conduct authorised by section 41 which is not conduct by an intercepting authority (within the meaning given by section 2).

(4) In keeping matters under review in accordance with this section, the Investigatory Powers Commissioner must, in particular, keep under review the operation of safeguards to protect privacy.

(5) In exercising functions under this Act, the competent authority must not act in a way which the Investigatory Powers Commissioner considers to be contrary to the public interest or prejudicial to the-

- (a) security of Gibraltar;
- (b) prevention or detection of serious crime; or
- (c) economic well-being of Gibraltar.

(6) The Investigatory Powers Commissioner must, in particular, ensure that he does not-

- (a) jeopardise the success of an intelligence or security operation or a law enforcement operation;

- (b) compromise the safety or security of those involved; or
- (c) unduly impede the operational effectiveness of the Royal Gibraltar Police, HM Customs Gibraltar or a government department.

(7) Subsections (5) and (6) do not apply in relation to section 120(1) (error reporting).

(8) In this section-

"equipment data" has the same meaning as in Part 4 (see section 66);

"judicial authority" means a judge, court or tribunal or any person exercising the function of a judge, court or tribunal;

"related systems data" has the meaning given by section 18(5);

"relevant Minister" means a Minister of the Government of Gibraltar;

"secondary data" has the same meaning as in Part 2 (see section 19).

**Additional directed oversight functions.**

119.(1) So far as directed to do so by the Chief Minister and subject to subsection (2), the Investigatory Powers Commissioner must keep under review the carrying out of any aspect of the functions of-

- (a) the Royal Gibraltar Police;
- (b) HM Customs Gibraltar.

(2) Subsection (1) does not apply in relation to anything which is required to be kept under review by the Investigatory Powers Commissioner under section 118.

(3) The Chief Minister may give a direction under this section at the request of the Investigatory Powers Commissioner or otherwise.

(4) The Chief Minister must publish, in a manner which the Chief Minister considers appropriate, any direction under this section (and any revocation of such a direction) except so far as it appears to the Chief Minister that such publication would be contrary to the public interest or prejudicial to the-

- (a) security of Gibraltar;
- (b) prevention or detection of serious crime;
- (c) economic well-being of Gibraltar; or

- (d) continued discharge of the functions of any public authority whose activities include activities that are subject to review by the Investigatory Powers Commissioner.

### **Error Reporting.**

120.(1) The Investigatory Powers Commissioner must inform a person of any relevant error relating to that person of which he is aware if he considers that-

- (a) the error is a serious error; and
- (b) it is in the public interest for the person to be informed of the error.

(2) In making a decision under subsection (1)(a), the Investigatory Powers Commissioner may not decide that an error is a serious error unless the Commissioner considers that the error has caused significant prejudice or harm to the person concerned.

(3) Accordingly, the fact that there has been a breach of a person's right and freedom (within the meaning of the Gibraltar Constitution Order 2006) is not sufficient by itself for an error to be a serious error.

(4) In making a decision under subsection (1)(b), the Investigatory Powers Commissioner must, in particular, consider-

- (a) the seriousness of the error and its effect on the person concerned; and
- (b) the extent to which disclosing the error would be contrary to the public interest or prejudicial to the-
  - (i) security of Gibraltar;
  - (ii) prevention or detection of serious crime;
  - (iii) economic well-being of Gibraltar; or
  - (iv) continued discharge of the functions of any public authority.

(5) Before making a decision under subsection (1)(a) and (b), the Investigatory Powers Commissioner must ask the public authority which has made the error to make submissions to him about the matters concerned.

(6) When informing a person under subsection (1) of an error, the Investigatory Powers Commissioner must-

- (a) inform the person of any rights that the person may have to appeal to the Supreme Court on a point of law; and

- (b) provide such details of the error as the Commissioner considers to be necessary for the exercise of those rights, having regard in particular to the extent to which disclosing the details would be contrary to the public interest or prejudicial to anything falling within subsection (4)(b)(i) to (iv).

(7) The Investigatory Powers Commissioner may not inform the person to whom it relates of a relevant error except as provided by this section.

(8) A report under section 123(1) must include information about-

- (a) the number of relevant errors of which the Investigatory Powers Commissioner has become aware during the year to which the report relates;
- (b) the number of relevant errors which the Investigatory Powers Commissioner has decided during that year were serious errors; and
- (c) the number of persons informed under subsection (1) during that year.

(9) In this section "relevant error" means an error-

- (a) by a public authority in complying with any requirements which are imposed on it by virtue of this Act or any other enactment and which are subject to review by the Investigatory Powers Commissioner; and
- (b) of a description identified for this purpose in a code of practice which may be issued by the Minister under section 127,

and the Investigatory Powers Commissioner must keep under review the definition of "relevant error".

#### **Additional functions under this Part.**

121.(1) The Investigatory Powers Commissioner and the competent authority must give the Supreme Court all such documents, information and other assistance (including their opinion as to any appeal falling to be determined by the Supreme Court) as the Supreme Court may require-

- (a) in connection with the investigation of any matter by the Supreme Court; or
- (b) otherwise for the purposes of the Supreme Court's consideration or determination of any matter.

(2) The Investigatory Powers Commissioner and the competent authority may provide advice or information to any public authority or other person in relation to matters for which the Commissioner or the competent authority is responsible.

(3) But the Investigatory Powers Commissioner must consult the competent authority before providing any advice or information under subsection (2) if it appears to the Investigatory

Powers Commissioner that providing the advice or information might be contrary to the public interest or prejudicial to the-

- (a) security of Gibraltar;
- (b) prevention or detection of serious crime;
- (c) economic well-being of Gibraltar; or
- (d) continued discharge of the functions of any public authority whose activities include activities that are subject to review by the Investigatory Powers Commissioner.

**Functions under other Parts and other enactments.**

122. The Investigatory Powers Commissioner has the functions that are exercisable by him by virtue of any other Part of this Act or by virtue of any other enactment.

*Reports and investigation and information powers*

**Annual and other reports.**

123.(1) The Investigatory Powers Commissioner must, as soon as reasonably practicable after the end of each calendar year, make a report to the Chief Minister about the carrying out of the functions of the Commissioner and the competent authority.

(2) A report under subsection (1) must, in particular, include-

- (a) statistics on the use of the investigatory powers which are subject to review by the Investigatory Powers Commissioner (including the number of authorisations granted, considered or approved during the year);
- (b) information about the results of such use (including its impact);
- (c) information about the operation of the safeguards conferred by this Act in relation to items subject to legal privilege, confidential journalistic material and sources of journalistic information;
- (d) information about the following kinds of authorisations granted, considered or approved during the year-
  - (i) targeted interception authorisations referred to in section 20(2);
  - (ii) targeted equipment interference authorisations relating to matters within paragraph (b), (c), (e), (f), (g) or (h) of section 67(1); and

(iii) authorisations relating to directed surveillance, intrusive surveillance, covert human intelligence sources and entry on or interference with property and radiocommunication under Part 5; and

(e) the information on the errors required by virtue of section 120.

(3) The Investigatory Powers Commissioner must, at any time, make any report to the Chief Minister which has been requested by the Chief Minister.

(4) The Investigatory Powers Commissioner may, at any time, make any such report to the Chief Minister, on any matter relating to the functions of the Commissioner and the competent authority, as the Investigatory Powers Commissioner considers appropriate.

(5) A report under subsection (1) or (4) may, in particular, include such recommendations as the Investigatory Powers Commissioner considers appropriate about any matter relating to the functions of the Commissioner and the competent authority.

(6) On receiving a report from the Investigatory Powers Commissioner under subsection (1), the Chief Minister must-

(a) publish the report; and

(b) lay a copy of the published report before Parliament together with a statement as to whether any part of the report has been excluded from publication under subsection (7).

(7) The Chief Minister may, after consultation with the Investigatory Powers Commissioner, exclude from publication any part of a report under subsection (1) if, in the opinion of the Chief Minister, the publication of that part would be contrary to the public interest or prejudicial to the-

(a) security of Gibraltar;

(b) prevention or detection of serious crime;

(c) economic well-being of Gibraltar; or

(d) continued discharge of the functions of any public authority whose activities include activities that are subject to review by the Investigatory Powers Commissioner.

(8) The Investigatory Powers Commissioner may publish any report under subsection (3) or (4), or any part of such a report, if requested to do so by the Chief Minister.

(9) In this section “the Commissioner” means the Investigatory Powers Commissioner.

**Investigation and information powers.**

124.(1) The Investigatory Powers Commissioner may carry out such investigations, inspections and audits as he considers appropriate for the purposes of the Commissioner's functions.

(2) Every relevant person must disclose or provide to the Investigatory Powers Commissioner all such documents and information as the Commissioner may require for the purposes of the Commissioner's functions.

(3) Every relevant person must provide the Investigatory Powers Commissioner with such assistance as the Commissioner may require in carrying out any investigation, inspection or audit for the purposes of the Commissioner's functions.

(4) Assistance under subsection (3) may, in particular, include such access to apparatus, systems or other facilities or services as the Investigatory Powers Commissioner concerned may require in carrying out any investigation, inspection or audit for the purposes of the Commissioner's functions.

(5) An intercepting authority may report to the Investigatory Powers Commissioner any refusal by a telecommunications operator or postal operator to comply with any requirements imposed by virtue of this Act.

(6) A public authority must report to the Investigatory Powers Commissioner any relevant error (within the meaning given by section 120(9)) of which it is aware.

(7) In this section "relevant person" means-

- (a) any person who holds, or has held, an office, rank or position with a public authority;
- (b) any telecommunications operator or postal operator who is, has been or may become subject to a requirement imposed by virtue of this Act; or
- (c) any person who is, has been or may become subject to a requirement to provide assistance by virtue of section 36, 38, 79, 81 or section 108.

(8) In this section "the Commissioner" means the Investigatory Powers Commissioner.

**Information gateway.**

125.(1) A disclosure of information to the Investigatory Powers Commissioner for the purposes of any function of the Commissioner does not breach-

- (a) an obligation of confidence owed by the person making the disclosure; or

(b) any other restriction on the disclosure of information (whether imposed by virtue of this Act or otherwise).

(2) But subsection (1) does not apply to a disclosure, in contravention of any provisions of the data protection legislation, of personal data which is not exempt from those provisions.

(3) In this section “data protection legislation” has the meaning given to it under section 2 of the Data Protection Act 2004

(4) In this section “the Commissioner” means the Investigatory Powers Commissioner.

*Supplementary provision*

**Power to modify functions.**

126.(1) The Minister may by regulations modify the functions of the Investigatory Powers Commissioner.

(2) The power to make regulations under this section (including that power as extended by section 139(1)(b)) may, in particular, be exercised by modifying any provision made by or under an enactment (including this Act).

**Chapter 2**

**Other Arrangements**

*Codes of practice*

**Codes of practice.**

127.(1) The Minister may issue one or more codes of practice relating to the exercise and performance of powers and duties conferred by virtue of this Act.

(2) Subsection (1) does not apply in relation to-

(a) any functions conferred by virtue of this Act on-

(i) the Investigatory Powers Commissioner; or

(ii) any other court;

(b) any function to make subsidiary legislation which is conferred by virtue of this Act on the Minister.

(3) A code of practice must be published and comes into operation on the date of publication.

(4) A person exercising or performing any power or duty in relation to which provision may be made by a code or practice under this section must, in doing so, have regard to the provisions (so far as they are applicable) of every code of practice for the time being in force under this section.

(5) A failure on the part of any person to comply with any provision of a code of practice issued under this section does not of itself render him liable to any criminal or civil proceedings but may be taken into account in deciding on the admissibility and weight of any evidence obtained in contravention of the provision.

(6) A code of practice issued under this section is admissible in evidence in any criminal or civil proceedings.

(7) The Minister may from time to time review a code of practice previously brought into operation under this section and the preceding provisions of this section apply to a revised code of practice as they apply to the code of practice as first prepared.

### **Chapter 3**

#### **Appeals**

#### **Appeals to Court of Appeal.**

128. A decision of the Supreme Court under this Act is final, but an appeal lies to the Court of Appeal where-

- (a) the appeal would raise an important point of principle or practice; or
- (b) there is another compelling reason for granting leave.

### **PART 8**

#### **Miscellaneous and General Provisions**

#### **Chapter 1 Miscellaneous**

#### *Urgent authorisations*

#### **Urgent authorisation granted by an intercepting authority.**

129.(1) This section applies where-

- (a) it is not possible to make an application to the competent authority for the grant of an authorisation under this Act;

(b) the matter is urgent; and

(c) there is an imminent threat to life or it is in the interests of the security of Gibraltar.

(2) Where subsection (1) applies an intercepting authority has the power to grant an urgent authorisation and allow the taking of such action as it may specify in accordance with the provisions of this Act.

(3) An intercepting authority shall not grant an urgent authorisation under subsection (2) unless it believes that the taking of the action is proportionate to what the action seeks to achieve and could not reasonably be achieved by other means.

**Notification of urgent authorisation to competent authority.**

130.(1) Where an intercepting authority grants an urgent authorisation under section 129, it must seek approval from the competent authority for the urgent authorisation.

(2) Pursuant to subsection (1) an intercepting authority must within 24 hours from when the urgent authorisation was granted by them, give notice in writing to the competent authority seeking approval of the said grant of urgent authorisation.

(3) When the competent authority receives notice from an intercepting authority seeking approval of the urgent authorisation, the competent authority must consider the notice and shall—

(a) grant approval of the urgent authorisation and add further conditions as it deems necessary; or

(b) refuse approval of the urgent authorisation;

and shall give written notice of its decision to the intercepting authority who granted the urgent authorisation.

(4) Where the competent authority refuses to approve the urgent authorisation, the urgent authorisation ceases to have effect and all material obtained pursuant to it shall be destroyed forthwith in accordance with arrangements made with the competent authority.

(5) The competent authority shall approve an urgent authorisation if, and only if, it is satisfied that there are reasonable grounds for believing the matters specified in section 129(3) are met.

(6) Where the competent authority approves an urgent authorisation granted under section 129, the urgent authorisation shall have effect from the time it was granted by the intercepting authority.

(7) Pursuant to this Act, the same provisions in relation to duration and appeal continue to apply to urgent authorisations as they do to non-urgent authorisations.

*The competent authority*

**The competent authority.**

131.(1) The Governor must appoint a competent authority, in consultation with the Chief Minister, acting on the advice of the Judicial Services Commission.

(2) A person is not to be appointed as the competent authority unless-

(a) the person holds or has held a high judicial office; or

(b) is among persons recommended by-

(i) the Chief Minister; or

(ii) the Governor.

(3) The competent authority may, to such extent as necessary, with approval from the Governor, delegate his functions in writing to such person as is suitably qualified and only where he-

(a) is away from the jurisdiction; or

(b) cannot, during a period of time, discharge the functions of his office due to illness or other inability.

(4) The delegation under subsection (3) to any extent of functions by the competent authority does not prevent the exercise of the functions to that extent by that competent authority.

**Terms and conditions of appointment.**

132.(1) Subject as follows, the competent authority holds and vacates office in accordance with the competent authority's terms and conditions of appointment.

(2) The competent authority is to be appointed for a term of three years.

(3) A person who ceases to be the competent authority (otherwise than under subsection (5)) may be re-appointed under section 131(1).

(4) The competent authority may not, subject to subsection (5), be removed from office before the end of the term for which the competent authority is appointed.

(5) The competent authority may be removed from office by the Governor, acting with the agreement of the Chief Minister, for inability to discharge the functions of his office (whether arising from infirmity of body or mind or any other cause) or for misbehaviour.

*Combined authorisations and notices*

**Combination of authorisations and notices.**

133. Schedule 3 (which makes provision for the combination of certain authorisations and notices in a single instrument) has effect.

*Compliance with Act*

**Payments towards certain compliance costs.**

134.(1) The Minister with responsibility for Finance must ensure that arrangements are in force for securing that telecommunications operators and postal operators receive an appropriate contribution in respect of such of their relevant costs as the Minister with responsibility for Finance considers appropriate.

(2) In subsection (1) "relevant costs" means costs incurred, or likely to be incurred, by telecommunications operators and postal operators in complying with this Act.

(3) The arrangements may provide for payment of a contribution to be subject to terms and conditions determined by the Minister with responsibility for Finance.

(4) Such terms and conditions may, in particular, include a condition on the operator concerned to comply with any audit that may reasonably be required to monitor the claim for costs.

(5) The arrangements may provide for the Minister with responsibility for Finance to determine-

(a) the scope and extent of the arrangements; and

(b) the appropriate level of contribution which should be made in each case.

(6) Different levels of contribution may apply for different cases or descriptions of case but the appropriate contribution must never be nil.

(7) For the purpose of complying with this section the Minister with responsibility for Finance may make, or arrange for the making of, payments out of money from the Consolidated Fund.

**Power to develop compliance systems etc.**

135.(1) The Minister with responsibility for Finance may-

(a) develop, provide, maintain or improve; or

- (b) enter into financial or other arrangements with any person for the development, provision, maintenance or improvement of,

such apparatus, systems or other facilities or services as the Minister with responsibility for Finance considers appropriate for enabling or otherwise facilitating compliance by the Minister with responsibility for Finance, another public authority or any other person with this Act.

(2) Arrangements falling within subsection (1)(b) may, in particular, include arrangements consisting of the giving of financial assistance by the Minister with responsibility for Finance.

(3) Such financial assistance-

- (a) may, in particular, be given by way of-

- (i) grant;
- (ii) loan;
- (iii) guarantee or indemnity;
- (iv) investment; or
- (v) incurring expenditure for the benefit of the person assisted; and

- (b) may be given subject to terms and conditions determined by the Minister with responsibility for Finance .

(4) Terms and conditions imposed by virtue of subsection (3)(b) may include terms and conditions as to repayment with or without interest.

### **Foreign surveillance operations (“continued surveillance”).**

136.(1) This section applies where-

- (a) a foreign officer is carrying out continued surveillance outside Gibraltar which is lawful under the law of the country or territory in which it is being carried out;
- (b) circumstances arise by virtue of which the surveillance can for the time being be carried out only in Gibraltar; and
- (c) it is not reasonably practicable in those circumstances for a Gibraltar officer to carry out the surveillance in Gibraltar in accordance with an authorisation under Part 5.

(2) “Continued surveillance” means surveillance which-

- (a) is carried out in relation to a person who is suspected of having committed a relevant crime or a person under surveillance who can assist in identifying or tracing such a person; and
- (b) is, for the purposes of Part 5, directed surveillance.

(3) This section shall apply to a foreign officer of a country or territory that has entered into an administrative arrangement that is applicable between that country or territory and Gibraltar, containing obligations on continued surveillance.

(4) For the purposes of this section, Schedule 6 sets out the-

- (a) country or territory that has entered into an administrative arrangement that is applicable between that country or territory and Gibraltar on continued surveillance;
- (b) conditions under which continued surveillance may be lawfully carried out on a reciprocal basis by a foreign officer and by a Gibraltar officer under the terms of the administrative arrangement on continued surveillance; and
- (c) lists the criminal offences falling under “relevant crime” for the purposes of that administrative arrangement.

(5) In this section, references to a foreign officer are to an officer who, in relation to a country or territory other than Gibraltar, is an officer for the purposes of any administrative arrangement to which Gibraltar is a party.

(6) In this section “Gibraltar officer” means a police officer;

## **Chapter 2**

### **General**

#### *Supplementary provision*

#### **Offences by bodies corporate etc.**

137.(1) This section applies if an offence under this Act is committed by a body corporate.

(2) If the offence is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of-

- (a) a senior officer of the body corporate; or
- (b) a person purporting to act in such a capacity,

the senior officer or person (as well as the body corporate or partnership) is guilty of the offence and liable to be proceeded against and punished accordingly.

(3) In this section-

"director", in relation to a body corporate whose affairs are managed by its members, means a member of the body corporate;

"senior officer" means a director, manager, secretary or other similar officer of the body corporate.

### **Territorial application of this Act.**

138.(1) If-

- (a) no act or omission which forms part of an offence under this Act takes place in Gibraltar;
- (b) a person's acts or omissions done or made outside Gibraltar would form part of such an offence if done or made in Gibraltar; and
- (c) that person has a close connection with Gibraltar,

proceedings for the offence may be taken in Gibraltar.

(2) An offence can be committed under this Act whether the acts or omissions which form part of the offence take place in Gibraltar or elsewhere.

(3) For the purposes of subsection (1), a person has a close connection with Gibraltar if at the time when the acts or omissions were done or made, the person was-

- (a) an individual who is Gibraltarian, a Gibraltar resident or who at the time of committing the offence was a Gibraltarian or Gibraltar resident; or
- (b) a body incorporated under the law of Gibraltar.

### **Regulations and Orders.**

139.(1) Any power of the Minister to make regulations or orders under this Act-

- (a) may be exercised so as to make different provision for different purposes or different areas; and
- (b) includes power to make supplementary, incidental, consequential, transitional, transitory or saving provision.

(2) See section 127 for the procedure about the coming into force of a code of practice under that section or of any revisions to such a code of practice.

(3) The Minister may by regulations amend the Schedules to this Act as he considers appropriate.

**Financial provisions.**

140. There is to be paid out of money provided from the Consolidated Fund-

- (a) any expenditure incurred by a Minister or government department by virtue of this Act; and
- (b) any increase attributable to this Act in the sums payable by virtue of any other Act out of money so provided.

**Transitional, transitory or saving provision.**

141.(1) The Minister may by regulations make such transitional, transitory or saving provision as the Minister considers appropriate in connection with the coming into force of any provision of this Act.

*General saving for lawful conduct*

(2) Nothing in any of the provisions of this Act by virtue of which conduct of any description is or may be authorised by any authorisation or notice, or by virtue of which information may be obtained in any manner, is to be read-

- (a) as making it unlawful to engage in any conduct of that description which is not otherwise unlawful under this Act and would not be unlawful apart from this Act;
- (b) as otherwise requiring-
  - (i) the grant of such an authorisation or notice; or
  - (ii) the taking of any step for or towards obtaining the authority of such an authorisation or notice;

before any such conduct of that description is engaged in, or

- (c) as prejudicing any power to obtain information by any means not involving conduct that may be authorised under this Act.

**Minor and consequential provision.**

142.(1) The Minister may by regulations make such provision as he considers appropriate in consequence of this Act.

(2) The power to make regulations under subsection (1) may, in particular, be exercised by modifying any provision made by or under an enactment.

(3) The Government may by regulations amend any Act or subsidiary legislation in order to make further provision for investigatory powers and generally in order to make such consequential, transitional and saving provisions as it deems necessary for the purpose of giving effect to this Act.

## **SCHEDULE 1**

### **Monetary Penalty Notices**

#### **Section 12**

##### **Part 1**

### **Monetary Penalty Notices**

#### *Payment of monetary penalties*

1.(1) A monetary penalty imposed by a monetary penalty notice must be paid to the competent authority within the period specified in the notice.

(2) The period specified under sub-paragraph (1) must not be less than 28 days beginning with the day after the day on which the notice is served.

(3) Any sum received by the competent authority by virtue of a monetary penalty notice must be paid into the Consolidated Fund.

#### *Contents of monetary penalty notices*

2. A monetary penalty notice must, in particular-

- (a) state the name and address of the person on whom it is to be served;
- (b) provide details of the notice of intent served on that person (see paragraph 4);
- (c) state whether the competent authority has received written representations in accordance with that notice of intent;
- (d) state the grounds on which the competent authority serves the monetary penalty notice;
- (e) state the grounds on which the competent authority decided the amount of the monetary penalty imposed by the monetary penalty notice;
- (f) state the details of how the monetary penalty is to be paid;
- (g) provide details of the person's rights of appeal under paragraph 8 in respect of the monetary penalty notice;
- (h) provide details of the competent authority's rights of enforcement under paragraph 9 in respect of the monetary penalty notice.

*Enforcement obligations*

3.(1) The competent authority may include an enforcement obligation, or enforcement obligations, in a monetary penalty notice if the competent authority considers that the interception to which the notice relates is continuing.

(2) Each of the following is an enforcement obligation-

- (a) a requirement on the person on whom the notice is served to cease the interception on a specified day or within a specified period;
- (b) (where appropriate for achieving such a cessation) a requirement on the person to take specified steps within a specified period, or to refrain from taking specified steps after the end of a specified period.

(3) An enforcement obligation may not have effect before the end of the period of 7 days beginning with the day after the day on which the notice is served.

(4) Where an enforcement obligation is included in a monetary penalty notice under this paragraph, the notice must state what the obligation is and the grounds for including it.

*Consultation requirements before service of monetary penalty notices*

4.(1) The competent authority must proceed in accordance with sub-paragraphs (2) to (7) before serving a monetary penalty notice on a person.

(2) The competent authority must serve a notice of intent on the person.

(3) A notice of intent is a notice that the competent authority proposes to serve a monetary penalty notice on the person.

(4) A notice of intent served on a person must, in particular-

- (a) state the name and address of the person;
- (b) state the grounds on which the competent authority proposes to serve the monetary penalty notice;
- (c) provide an indication of the amount of the monetary penalty that the competent authority proposes to impose and the competent authority's grounds for deciding that amount;
- (d) state whether the monetary penalty notice is to include any enforcement obligation and, if so, what the obligation is and the grounds for including it;
- (e) state the date on which the competent authority proposes to serve the monetary penalty notice;

- (f) inform the person that the person may make written representations in relation to the competent authority's proposal within a period specified in the notice; and
- (g) inform the person that they may, within a period specified in the notice, request an oral hearing before the competent authority in order to make representations of the kind mentioned in sub-paragraph (6)(b).

(5) No period specified as mentioned in sub-paragraph (4)(f) or (g) may be less than 21 days beginning with the day after the day on which the notice is served.

(6) Where the person has requested an oral hearing within the period specified for the purpose in the notice-

- (a) the competent authority must arrange such a hearing; and
- (b) the person may make representations at the hearing about-
  - (i) any matter falling within section 8(3)(c); or
  - (ii) any other matter relating to the competent authority's proposal which, by virtue of section 50, the person would be unable to raise on an appeal under paragraph 8.

(7) The competent authority must consider any representations which have been made by the person in accordance with the notice or sub-paragraph (6).

(8) If the competent authority decides not to serve a monetary penalty notice on a person as a result of any representations which have been made by the person in accordance with a notice of intent or sub-paragraph (6), the competent authority must inform the person of that fact.

5.(1) The competent authority may not vary a notice of intent except as set out in sub-paragraph (2).

(2) The competent authority may vary a notice of intent by extending the period mentioned in paragraph 4(4)(f) or (g).

(3) Sub-paragraph (1) does not prevent the competent authority from serving a new notice of intent instead of varying such a notice.

(4) The competent authority may cancel a notice of intent.

(5) A variation or cancellation of a notice of intent is effected by serving on the person on whom the notice was served a notice setting out the variation or cancellation.

6.(1) The competent authority must not serve a monetary penalty notice on a person in respect of an interception if any notice of intent in respect of that interception was served on the person more than 3 months earlier.

(2) But the competent authority may serve a monetary penalty notice on a person where the service of the notice would otherwise be prevented by sub-paragraph (1) if the competent authority-

- (a) considers it reasonable to do so; and
- (b) includes the reasons for doing so in the monetary penalty notice.

*Variation or cancellation of monetary penalty notices*

7.(1) The competent authority may vary or cancel a monetary penalty notice.

(2) But the competent authority may not vary a monetary penalty notice in a way that is detrimental to the person on whom it was served (whether by increasing the amount of the monetary penalty, by reducing the period specified in the notice as the period within which the penalty must be paid, by imposing a new enforcement obligation or making an existing enforcement obligation effective earlier or otherwise more onerous, or otherwise).

(3) The competent authority must-

- (a) in the case of a variation which reduces the amount of a monetary penalty, repay any excess already paid in accordance with the notice; and
- (b) in the case of a cancellation, repay any amount already paid in accordance with the notice.

(4) A variation or cancellation of a monetary penalty notice is effected by serving on the person on whom the monetary penalty notice was served a notice setting out the variation or cancellation.

(5) The competent authority may not serve another monetary penalty notice on a person in respect of an interception if the competent authority has cancelled a previous notice served on the person in respect of the same interception.

(6) If the competent authority refuses a request by a person to vary or cancel a monetary penalty notice which has been served on the person, the competent authority must inform the person of that fact.

*Appeals in relation to monetary penalty notices*

8.(1) A person on whom a monetary penalty notice is served may appeal to the Supreme Court against-

- (a) the monetary penalty notice or any provision of it; or
- (b) any refusal of a request by the person to serve a notice of variation or cancellation in relation to the monetary penalty notice.

(2) Where there is an appeal under sub-paragraph (1)(a) in relation to a monetary penalty notice or any provision of it, any requirement in the notice or (as the case may be) provision which does not relate to the imposition of an enforcement obligation need not be complied with until the appeal is withdrawn or finally determined.

(3) Sub-paragraphs (4) to (6) apply in relation to an appeal under sub-paragraph (1)(a).

(4) The Supreme Court must allow the appeal or substitute such other monetary penalty notice as could have been served by the competent authority if the Supreme Court considers-

- (a) that the notice to which the appeal relates is not in accordance with the law; or
- (b) to the extent that the notice involved an exercise of discretion by the competent authority, that the competent authority ought to have exercised the discretion differently.

(5) In any other case, the Supreme Court must dismiss the appeal.

(6) The Supreme Court may review any determination of fact on which the notice was based.

(7) Sub-paragraphs (8) to (10) apply in relation to an appeal under sub-paragraph (1)(b).

(8) The Supreme Court must direct the competent authority to serve, on such terms as the Supreme Court considers appropriate, a notice of variation or cancellation in relation to the monetary penalty notice if the Supreme Court considers that the monetary penalty notice ought to be varied or cancelled on those terms.

(9) In any other case, the Supreme Court must dismiss the appeal.

(10) The Supreme Court may review any determination of fact on which the refusal to serve the notice of variation or cancellation was based.

#### *Enforcement of monetary penalty notices*

9. In relation to any penalty payable to the competent authority by virtue of a monetary penalty notice, the penalty is recoverable as if it were payable under an order of that court.

10.(1) A person on whom a monetary penalty notice containing an enforcement obligation is served must comply with the obligation.

(2) The duty imposed by sub-paragraph (1) is enforceable by civil proceedings by the competent authority for an injunction or for any other appropriate relief.

*Guidance*

11.(1) The competent authority may prepare and grant guidance on how the competent authority proposes to exercise the competent authority's functions under section 12 and this Schedule.

(2) The guidance must, in particular, deal with-

- (a) the manner in which the competent authority is to deal with claims of a description specified in the guidance which may give rise to grounds for serving a monetary penalty notice;
- (b) the circumstances in which the competent authority would consider it appropriate to serve a monetary penalty notice;
- (c) how the competent authority will determine the amount of the penalty; and
- (d) the circumstances in which the competent authority would consider it appropriate to impose an enforcement obligation.

(3) The competent authority may alter or replace the guidance.

(4) If the guidance is altered or replaced, the competent authority must issue the altered or replacement guidance.

(5) The competent authority must arrange for the publication, in such form and manner as the competent authority considers appropriate, of any guidance issued under this paragraph.

*Interpretation of Part 1*

12. In this Part of this Schedule-

"address" means-

- (a) in the case of a registered company, the address of its registered office;
- (b) in the case of a person (other than a registered company) carrying on a business, the address of the person's principal place of business in Gibraltar; and
- (c) in any other case, the person's last known address;

"enforcement obligation" has the meaning given by paragraph 3(2);

"monetary penalty notice" means a monetary penalty notice under section 8;

"notice" means notice in writing;

"notice of intent" has the meaning given by paragraph 4(3);

"registered company" means a company registered under the enactments relating to companies for the time being in force in Gibraltar.

## **Part 2**

### **Information Provisions**

#### *Information notices*

13.(1) The competent authority may by notice (an "information notice") request any person on whom the competent authority is considering whether to serve a Part 1 notice of intent or a Part 1 monetary penalty notice to provide such information as the competent authority reasonably requires for the purpose of deciding whether to serve it.

(2) Where the competent authority requests that documents be produced, the competent authority may take copies of, or extracts from, any document so produced.

(3) An information notice must-

- (a) specify or describe the information to be provided;
- (b) specify the manner in which, and the period within which, the information is to be provided;
- (c) state that the competent authority considers that the information is information which the competent authority reasonably requires for the purpose of deciding whether to serve a Part 1 notice of intent or (as the case may be) a Part 1 monetary penalty notice;
- (d) state the competent authority's grounds for this view; and
- (e) provide details of the rights of appeal under paragraph 15 in respect of the information notice.

(4) For the purposes of sub-paragraph (3)(b)-

- (a) specifying the manner in which the information is to be provided may include specifying the form in which it is to be provided; and
- (b) the specified period within which the information is to be provided must not be less than 28 days beginning with the day after the day on which the information notice is served.

14.(1) The competent authority may not vary an information notice except as set out in sub-paragraph (2).

(2) The competent authority may vary an information notice by extending the period within which the information is to be provided if the person on whom the notice is served appeals under paragraph 15 in relation to the notice.

(3) Sub-paragraph (1) does not prevent the competent authority from serving a new information notice instead of varying such a notice.

(4) The competent authority may cancel an information notice.

(5) A variation or cancellation of an information notice is effected by serving on the person on whom the notice was served a notice setting out the variation or cancellation.

*Appeals in relation to information notices*

15.(1) A person on whom an information notice is served may appeal to the Supreme Court against-

- (a) the information notice or any provision of it; or
- (b) any refusal of a request by the person to serve a notice of variation or cancellation in relation to the information notice.

(2) Subject to paragraph 14(2), an appeal under this paragraph does not affect the need to comply with the information notice while the appeal has not been withdrawn or finally determined.

(3) Sub-paragraphs (4) to (6) apply in relation to an appeal under sub-paragraph (1)(a).

(4) The Supreme Court must allow the appeal or substitute such other information notice as could have been served by the competent authority if the Supreme Court considers-

- (a) that the notice to which the appeal relates is not in accordance with the law; or
- (b) to the extent that the notice involved an exercise of discretion by the competent authority, that the competent authority ought to have exercised the discretion differently.

(5) In any other case, the Supreme Court must dismiss the appeal.

(6) The Supreme Court may review any determination of fact on which the notice was based.

(7) Sub-paragraphs (8) to (10) apply in relation to an appeal under sub-paragraph (1)(b).

(8) The Supreme Court must direct the competent authority to grant, on such terms as the Supreme Court considers appropriate, a notice of variation or cancellation in relation to the information notice if the Supreme Court considers that the information notice ought to be varied or cancelled on those terms.

(9) In any other case, the Supreme Court must dismiss the appeal.

(10) The Supreme Court may review any determination of fact on which the refusal to serve the notice of variation or cancellation was based.

#### *Enforcement of information notices*

16.(1) The competent authority may serve a Part 2 monetary penalty notice on a person if the person-

- (a) without reasonable excuse fails to comply with an information notice; or
- (b) knowingly or recklessly gives any information which is false in a material particular in response to an information notice.

(2) A Part 2 monetary penalty notice is a notice requiring the person on whom it is served to pay to the competent authority a monetary penalty of an amount determined by the competent authority and specified in the notice.

(3) The amount of a monetary penalty determined by the competent authority under this paragraph may be-

- (a) a fixed amount;
- (b) an amount calculated by reference to a daily rate; or
- (c) a fixed amount and an amount calculated by reference to a daily rate.

(4) But the total amount payable must not exceed £10,000.

(5) In the case of an amount calculated by reference to a daily rate-

- (a) no account is to be taken of the day on which the Part 2 monetary penalty notice is served or any day before that day; and
- (b) the Part 2 monetary penalty notice must specify-
  - (i) the day on which the amount first starts to accumulate and the circumstances in which it is to cease to accumulate; and
  - (ii) the period or periods within which the amount, or any part or parts so far accumulated, must be paid to the competent authority.

Any period falling within paragraph (b)(ii) must not be less than 28 days beginning with the day after the day on which the notice is served.

17.(1) Part 1 of this Schedule applies in relation to a Part 2 monetary penalty notice and the penalty that relates to that notice as it applies in relation to a Part 1 monetary penalty notice and the penalty that relates to that notice.

(2) The provisions in Part 1 of this Schedule so far as relating to enforcement obligations do not apply in relation to a Part 2 monetary penalty notice.

(3) Paragraph 4 has effect in relation to a Part 2 monetary penalty notice as if in sub-paragraph (6)(b) the reference to making representations about matters falling within sub-paragraph (6)(b)(i) or (ii) were a reference to making representations about matters falling within sub-paragraph (6)(b)(ii) only.

(4) Paragraph 6 has effect in relation to a Part 2 monetary penalty notice as if the references in sub-paragraph (1) to an interception were references to conduct falling within paragraph 16(1)(a) or (b).

(5) Paragraph 7(5) has effect in relation to a Part 2 monetary penalty notice as if the references to an interception were references to conduct falling within paragraph 16(1)(a) or (b).

#### *Technical assistance for the competent authority*

18.(1) The GRA must comply with any reasonable request made by the competent authority, in connection with the competent authority's functions under section 8 and this Schedule, for advice on technical and similar matters relating to electronic communications.

(2) For this purpose, the competent authority may disclose to the GRA any information obtained by the competent authority under this Schedule.

(3) In this paragraph "GRA" means the Gibraltar Regulatory Authority established by section 3 of the Gibraltar Regulatory Authority Act 2000.

#### *Interpretation of Part 2*

19. In this Part of this Schedule-

"enforcement obligation" has the meaning given by paragraph 3(2);

"information" includes documents; and any reference to providing or giving information includes a reference to producing a document;

"information notice" has the meaning given by paragraph 13(1);

"notice" means notice in writing;

"Part 1 monetary penalty notice" means a monetary penalty notice under section 8;

"Part 1 notice of intent" means a notice of intent (within the meaning of paragraph 4(3)) relating to a Part 1 monetary penalty notice;

"Part 2 monetary penalty notice" means a monetary penalty notice under paragraph 16.

## **SCHEDULE 2**

### **Exceptions to section 49**

#### **Section 49**

#### ***Introductory***

1. This Schedule contains-

- (a) exceptions to the exclusion by section 49(1) of certain matters from legal proceedings; and
- (b) limitations on those exceptions where that exclusion will still apply.

#### ***Disclosures of lawfully intercepted communications***

2.(1) Section 49(1)(a) does not prohibit the disclosure of any content of a communication, or any secondary data obtained from a communication, if the interception of that communication was lawful by virtue of sections 11(1)(c) and 39 to 45.

(2) Where any disclosure is proposed to be, or has been, made on the grounds that it is authorised by sub-paragraph (1), section 49(1) does not prohibit the doing of anything in, or for the purposes of, so much of any proceedings as relates to the question whether that disclosure is or was so authorised.

#### ***Disclosures of convictions for certain offences***

3. Section 49(1)(b) does not prohibit the doing of anything that discloses any conduct of a person for which that person has been convicted of an offence under section 8(1), 38(6) or 52.

#### ***Proceedings before the Supreme Court***

4. Section 49(1) does not apply in relation to-

- (a) any proceedings before the Supreme Court; or
- (b) any proceedings arising out of such an appeal.

#### ***Proceedings before Proscribed Organisations Appeal Commission***

5.(1) Section 49(1) does not apply in relation to-

- (a) any proceedings before the Proscribed Organisations Appeal Commission; or
- (b) any proceedings arising out of proceedings before that Commission.

(2) But sub-paragraph (1) does not permit the disclosure of anything to any of the following-

- (a) the applicant to the Commission;
- (b) the organisation concerned (if different);
- (c) any person who represents that appellant or that organisation for the purposes of the proceedings.

*Employment tribunal proceedings*

6.(1) Section 49(1) does not apply in relation to any proceedings before an employment tribunal where the applicant, or the applicant's representatives, are excluded for all or part of the proceedings pursuant to-

- (a) a direction to the tribunal by virtue of rule 77 of the Employment Tribunal (Constitution and Procedure) Rules 2016 (National security proceedings); or
- (b) a determination of the tribunal by virtue of rule 44 of those Rules (Privacy and restrictions on disclosure).

(2) Section 49(1) does not apply in relation to any proceedings arising out of proceedings within sub-paragraph (1).

7. But paragraph 6 does not permit the disclosure of anything to-

- (a) the person who is or was the applicant in the proceedings before the employment or industrial tribunal; or
- (b) any person who-
  - (i) represents that person for the purposes of any proceedings within paragraph 6; and
  - (ii) does so otherwise than by virtue of appointment as a special advocate.

*Proceedings relating to dismissal for certain offences*

8. Section 49(1) does not prohibit anything done in, for the purposes of, or in connection with, so much of any legal proceedings as relates to the fairness or unfairness of a dismissal on any conduct constituting an offence under section 8(1), 38(6) or 52

*Civil proceedings for enforcement of duty to assist with implementation of authorisations*

9. Section 49(1) does not apply in relation to any civil proceedings under section 38(7) of this Act.

*Proceedings for certain offences*

10.(1) Section 49(1) does not apply in relation to any proceedings for a relevant offence.

(2) "Relevant offence" means-

- (a) an offence under any provision of this Act;
- (b) an offence under section 76 of the Communications Act 2006;
- (c) an offence under section 29, 30, 32, 35 of the Post Office Act;
- (d) an offence under section 1 or 2 of the Official Secrets Act 1911 relating to any sketch, plan, model, article, note, document or information which-
  - (i) incorporates, or relates to, the content of any intercepted communication or any secondary data obtained from a communication; or
  - (ii) tends to suggest that any interception-related conduct has or may have occurred or may be going to occur;
- (e) an offence of perjury committed in the course of any relevant proceedings;
- (f) an offence of attempting or conspiring to commit an offence falling within any of paragraphs (a) to (e);
- (g) an offence under section 36 of the Crimes Act 2011 in relation to an offence within any of those paragraphs;
- (h) an offence of aiding, abetting, counselling or procuring the commission of an offence falling within any of those paragraphs;
- (i) contempt of court committed in the course of, or in relation to, any relevant proceedings.

(3) In this paragraph-

"intercepted communication" and "interception-related conduct" have the same meaning as in section 49;

"relevant proceedings" means any proceedings mentioned in paragraphs 4 to 9.

*Disclosures to prosecutors and judges*

11.(1) Nothing in section 49(1) prohibits-

- (a) a disclosure to a person ("P") conducting a criminal prosecution that is made for the purpose only of enabling P to determine what is required of P by P's duty to secure the fairness of the prosecution; or
- (b) a disclosure to a relevant judge in a case in which the judge has ordered the disclosure to be made to the judge alone.

(2) A relevant judge may order a disclosure under sub-paragraph (1)(b) only if the judge considers that the exceptional circumstances of the case make the disclosure essential in the interests of justice.

(3) Where in any criminal proceedings-

- (a) a relevant judge orders a disclosure under sub-paragraph (1)(b); and
- (b) in consequence of that disclosure, the judge considers that there are exceptional circumstances requiring the judge to make a direction under this sub-paragraph,

the judge may direct the person conducting the prosecution to make for the purposes of the proceedings any admission of fact which the judge considers essential in the interests of justice.

(4) But nothing in any direction under sub-paragraph (3) may authorise or require anything to be done in contravention of section 49(1).

(5) In this paragraph "relevant judge" means any judge of the Supreme Court.

#### *Disclosures to inquiries*

12.(1) Nothing in section 49(1) prohibits-

- (a) a disclosure to the panel of an inquiry held under the Inquiries Act 2024; or
- (b) a disclosure to a person appointed as legal adviser to such an inquiry,

where, in the course of the inquiry, the panel has ordered the disclosure to be made to the panel alone or (as the case may be) to the panel and any person appointed as legal adviser to the inquiry.

(2) The panel of an inquiry may order a disclosure under sub-paragraph (1) only if it considers that the exceptional circumstances of the case make the disclosure essential to enable the inquiry to fulfil its terms of reference.

(3) Any reference in this paragraph to a person appointed as legal adviser to an inquiry is a reference to a person appointed as solicitor or counsel to the inquiry.

### **SCHEDULE 3**

#### **COMBINATION OF AUTHORISATIONS AND NOTICES**

#### **Section 133**

##### **Part 1**

##### **Combinations with Targeted Interception Authorisations**

1. The competent authority may, on an application made by an intercepting authority, grant an authorisation that combines a targeted interception authorisation which the competent authority has power to grant under section 18(1), with one or more of the following-
  - (a) a targeted equipment interference authorisation under section 68;
  - (b) an authorisation under section 91 (directed surveillance);
  - (c) an authorisation under section 92 (intrusive surveillance);
  - (d) an authorisation under section 96A (entry on to or interference with property or with radiocommunication).

##### **Part 2**

##### **Combinations with Targeted Equipment Interference Authorisations**

2. The competent authority may, on an application made by an intercepting authority, grant an authorisation that combines a targeted equipment interference authorisation, which the competent authority has power to grant under section 68, with one or more of the following-
  - (a) an authorisation under section 91 (directed surveillance);
  - (b) an authorisation under section 92 (intrusive surveillance);
  - (c) an authorisation under section 96A (entry on to or interference with property or with radiocommunication).

### **Part 3**

#### **Combined Authorisations: Supplementary Provision**

##### *Introduction*

3. In this Part of this Schedule "combined authorisation" means an authorisation granted under any of Parts 1 or 2 of this Schedule.

##### *General*

(1) Where Parts 1 or 2 of this Schedule provides for the competent authority to have power, on an application made by an intercepting authority ("the applicant"), to grant a combined authorisation that includes any authorisation or other notice, the competent authority may grant a combined authorisation containing that authorisation or notice, whether or not the competent authority would have power, on an application made by the applicant, to grant that authorisation, as a single instrument.

(2) Where Parts 1 or 2 of this Schedule provides for an intercepting authority ("the applicant") to have power to apply for a combined authorisation, the applicant may apply for a combined authorisation containing any authorisation or other notice that may be included in it, provided that-

- (a) the applicant could apply for that authorisation or notice as a single instrument; or
- (b) the intercepting authority on whose behalf the person is acting, or another person who is a member of staff or an officer of the intercepting authority or who is otherwise acting on its behalf, could apply for that authorisation or notice as a single instrument.

4. A combined authorisation must be addressed to the intercepting authority who made the application for the combined authorisation.

5. A combined authorisation must contain a provision stating which authorisations or other notices are included in the combined authorisation.

6. Any reference in any enactment to an authorisation or other notice of a particular description granted or given under any enactment includes, in the case of a combined authorisation containing an authorisation or notice of that description, a reference to so much of the combined authorisation as consists of such an authorisation or notice.

This is subject to any provision made by or under the following provisions of this Schedule.

*Rules about grant etc. applying separately in relation to each part of a combined authorisation*

7.(1) The law about the following matters, so far as relating to an authorisation or other notice that may be included in a combined authorisation, applies in relation to so much of a combined authorisation as consists of such an authorisation or notice-

- (a) the duties imposed by section 7 (general duties in relation to privacy);
- (b) any conditions that must be met before such an authorisation or notice may be granted;
- (c) the grounds on which such an authorisation or notice may be granted;
- (d) the conduct that may be authorised by such an authorisation or notice;
- (e) any requirements as to what must be included in such an authorisation or notice;
- (f) any conditions that must be met before such an authorisation or notice may be renewed and the grounds on which it may be renewed;
- (g) any conditions that must be met before such an authorisation or notice may be modified;
- (h) the grounds on which such an authorisation or notice may be modified and the procedural rules that apply to such a modification;
- (i) the circumstances in which such an authorisation or notice may or must be cancelled.

(2) In sub-paragraph (1)(h) "procedural rules", in relation to the modification of an authorisation or other notice, means the law about any of the following matters-

- (a) the involvement of the competent authority in decisions;
- (b) the delegation of decisions;
- (c) the signing of instruments making a modification.

(3) Sub-paragraph (1) is subject to paragraphs 8 and 9.

*Rules about grant etc. applying in relation to combined authorisations*

8.(1) A combined authorisation under Part 1 of this Schedule addressed to any person may only be granted, renewed or cancelled in accordance with the procedural rules that would apply

to the grant, renewal or cancellation of a targeted interception authorisation addressed to that person (see Chapter 1 of Part 2 of this Act).

(2) In sub-paragraph (1) "procedural rules", in relation to an authorisation, means the law about any of the following matters-

- (a) the involvement of the competent authority in decisions;
- (b) the delegation of decisions;
- (c) the signing of authorisations.

9.(1) A combined authorisation under Part 2 of this Schedule addressed to any person may only be granted, renewed or cancelled in accordance with the procedural rules that would apply to the grant, renewal or cancellation of a targeted equipment interference authorisation addressed to that person (see Part 4 of this Act).

(2) In sub-paragraph (1) "procedural rules" has the same meaning as in paragraph 8(2).

#### *Modification of rules as to duration*

10.(1) Where a combined authorisation includes authorisations or notices which (as single instruments) would cease to have effect at the end of different periods, the combined authorisation is to cease to have effect at the end of the shortest of the periods (unless renewed).

(2) But sub-paragraph (1) does not apply to a combined authorisation which includes an authorisation of directed surveillance.

(3) In such a case, the combined authorisation (unless it is renewed) is to cease to have effect at the end of the period of 3 months beginning with the day on which it is granted.

#### *Special rules about the application of this Act to combined authorisations*

11.(1) This paragraph applies to any provision in Part 2 or 5 of this Act that enables a person to whom an authorisation is addressed to require the provision of assistance in giving effect to the authorisation.

(2) In the case of a combined authorisation containing such an authorisation, the provision is to be read as enabling the person to whom the combined authorisation is addressed to require the provision of assistance in giving effect to so much of the combined authorisation as consists of such an authorisation.

(3) Accordingly, any power to serve a copy of an authorisation for that purpose includes power, in the case of such a combined authorisation, to serve the part of the combined authorisation consisting of such an authorisation.

12. Any reference in section 49 (exclusion of matters from legal proceedings etc.) to the making of an application for an authorisation, or the grant of an authorisation, under Chapter 1 of Part 2 of this Act includes a reference to-

- (a) the making of an application for a combined authorisation that includes an authorisation under that Chapter, so far as relating to disclosing or suggesting the inclusion of such an authorisation; or
- (b) the inclusion of an authorisation under that Chapter in a combined authorisation.

13.(1) The reference in section 51(7) to the provisions of Part 2 of this Act is to be read, in the case of a combined authorisation containing a targeted interception authorisation which the person who granted the combined authorisation has power to grant under that Part, as including a reference to this Schedule.

(2) The reference in section 86(4) to the provisions of Part 4 of this Act is to be read, in the case of a combined authorisation containing a targeted equipment interference authorisation which the person who granted the combined authorisation has power to grant under that Part, as including a reference to this Schedule.

**SCHEDULE 4**

**TARGETED INTERCEPTION AUTHORISATION**

**MEMBERS OF PARLIAMENT, ETC. – ADDITIONAL SAFEGUARDS**

**Section 24**

**Part 1**

**Executive Member of Parliament or the Speaker of the House**

1.(1) This Part applies where-

- (a) an application is made under section 24 to the competent authority for the grant of a targeted interception authorisation; and
- (b) the purpose of the authorisation is to authorise or require the interception of communications sent by, or intended for, a person who is an executive Member of Parliament or the Speaker of the House.

(2) The competent authority may not grant an authorisation under this Part without the approval of-

- (a) the Chief Minister; or
- (b) if conditions A and B are met, the Deputy Chief Minister as designated in writing by the Chief Minister under this Part.

(3) Condition A is that the Chief Minister is unable to give approval under subparagraph (2).

(4) Condition B is that the competent authority or an intercepting authority, the latter pursuant to section 129, considers that there is an urgent need for the decision (as to whether to give such approval) to be made.

(5) A designation under this Part ends when revoked in writing by the Chief Minister.

(6) For the purposes of this Schedule “executive Member of Parliament” means a cabinet Minister, other than the Chief Minister.

## **Part 2**

### **Chief Minister**

2.(1) This Part applies where-

- (a) an application is made to the competent authority for the grant of a targeted interception authorisation; and
- (b) the purpose of the authorisation is to authorise or require the interception of communications sent by, or intended for, the Chief Minister.

(2) The competent authority may not grant an authorisation under this Part without the approval of the Deputy Chief Minister.

## **Part 3**

### **Non Executive Member of Parliament**

3.(1) This Part applies where-

- (a) an application is made to the competent authority for the grant of a targeted interception authorisation; and
- (b) the purpose of the authorisation is to authorise or require the interception of communications sent by, or intended for a non executive Member of Parliament.

(2) The competent authority may not grant an authorisation under this Part without the approval of the Speaker of the House.

(3) For the purposes of this Schedule “non executive Member of Parliament” means a member of Parliament, other than the Chief Minister, a cabinet Minister or the Speaker of the House.

## **SCHEDULE 5**

### **TARGETED EQUIPMENT INTERFERENCE AUTHORISATION**

#### **MEMBERS OF PARLIAMENT, ETC. – ADDITIONAL SAFEGUARDS**

#### **Section 70**

##### **Part 1**

##### **Executive Member of Parliament or the Speaker of the House**

##### **Members of Parliament, etc.**

1.(1) This Part applies where-

- (a) an application is made under section 68 to the competent authority by an intercepting authority for a targeted equipment interference authorisation; and
- (b) the purpose of the authorisation is to obtain-
  - (i) communications sent by, or intended for, a person who is an executive Member of Parliament or the Speaker of the House; or
  - (ii) an executive Member of Parliament's or Speaker of the House private information.

(2) The competent authority may not grant an authorisation under this Part without the approval of-

- (a) the Chief Minister; or
- (b) if conditions A and B are met, the Deputy Chief Minister as designated in writing by the Chief Minister under this Part.

(3) Condition A is that the Chief Minister is unable to give approval under subparagraph (2).

(4) Condition B is that the competent authority or an intercepting authority, the latter pursuant to section 129, considers that there is an urgent need for the decision (as to whether to give such approval) to be made.

(5) A designation under this Part ends when revoked in writing by the Chief Minister.

(6) For the purposes of this Schedule an "executive Member of Parliament" means a cabinet Minister, other than the Chief Minister.

## **Part 2**

### **Chief Minister**

2.(1) This Part applies where-

- (a) an application is made under section 68 to the competent authority by an intercepting authority for a targeted equipment interference authorisation; and
- (b) the purpose of the authorisation is to obtain-
  - (i) communications sent by, or intended for the Chief Minister; or
  - (ii) the Chief Minister's private information.

(2) The competent authority may not grant an authorisation under this Part without the approval of the Deputy Chief Minister.

## **Part 3**

### **Non Executive Member of Parliament**

3.(1) This Part applies where-

- (a) an application is made under section 68 to the competent authority by an intercepting authority for a targeted equipment interference authorisation; and
- (b) the purpose of the authorisation is to obtain-
  - (i) communications sent by, or intended for a non executive Member of Parliament; or
  - (ii) a non executive Member of Parliament's private information.

(2) The competent authority may not grant an authorisation under this Part without the approval of the Speaker of the House.

(3) For the purposes of this Schedule a "non executive Member of Parliament" means a member of Parliament, other than the Chief Minister, a cabinet Minister or the Speaker of the House.

## SCHEDULE 6

### CONDITIONS ON “CONTINUED SURVEILLANCE”

#### Section 136(4)

(A) Administrative Arrangement between the United Kingdom, in respect of Gibraltar and Spain on continued surveillance and uninterrupted pursuit.

1. Under the terms of the Administrative Arrangement referred to in subheading (A), the reciprocal conditions under which continued surveillance may be lawfully carried out by a foreign officer and by a Gibraltar officer (individually referred to as “the Participant” and collectively known as “the Participants”) are as follows-

- (a) The requesting Participant, who intends to carry out continued surveillance in Gibraltar or Spain, will inform, including via the encrypted radio frequency, the requested Participant as soon as possible and at the latest when they are about to enter the territory of the other Participant;
- (b) Should the requested Participant decide to take over the continued surveillance operation, they will communicate it, including through the shared encrypted radio frequency, and the continued surveillance of the requesting Participant who initiated it will thereupon cease;
- (c) The Participants carrying out the surveillance must comply with the Administrative Arrangement, with the law of Spain or Gibraltar, as the case may be, and they must obey the instructions of the competent local authorities;
- (d) The Participants carrying out the surveillance must at all times be able to prove that they are acting in an official capacity;
- (e) The Participants carrying out the surveillance may carry their service weapons during the surveillance save where specifically otherwise decided by the requested Participant; their use will be prohibited save in cases of legitimate self-defence;
- (f) Entry into private homes and places not accessible to the public will be prohibited to the requesting Participant;
- (g) The requesting Participant carrying out the surveillance may neither challenge nor arrest the person under surveillance;
- (h) All operations will be the subject of a report to the competent authorities of Spain, where the operations by Gibraltar officers took place in Spain, and to the competent authorities of Gibraltar, where the operations by foreign officers of Spain took place in Gibraltar. The officers carrying out the surveillance may be required to appear in person;

- (i) The requesting Participants who conducted the surveillance will, when so requested by the requested Participant, assist the enquiry subsequent to the operation in which they took part, including in judicial proceedings.

2. Criminal offences falling under the definition of “relevant crime” for the purposes of the Administrative Arrangement are-

- (a) terrorism
- (b) participation in a criminal organisation
- (c) murder and grievous bodily harm
- (d) manslaughter
- (e) organised or armed robbery
- (f) sexual exploitation of children and child pornography
- (g) rape
- (h) arson
- (i) computer-related crime
- (j) forgery of money
- (k) counterfeiting and piracy of products
- (l) forgery of administrative documents and trafficking therein
- (m) aggravated burglary and robbery and receiving stolen goods
- (n) corruption, including bribery
- (o) fraud
- (p) racketeering and extortion
- (q) swindling
- (r) laundering of the proceeds of crime
- (s) kidnapping, illegal restraint and hostage taking
- (t) trafficking in human beings
- (u) illicit trade in human organs and tissue
- (v) facilitation of unauthorised entry and residence
- (w) racism and xenophobia
- (x) illicit trafficking in narcotic drugs and psychotropic substances
- (y) illicit trafficking in cultural goods, including antiques and works of art
- (z) illicit trafficking in weapons, munition and explosives
- (aa) trafficking in stolen vehicles
- (bb) wilful damage through the use of explosives
- (cc) illicit transportation of toxic and hazardous waste
- (dd) environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties
- (ee) illicit trafficking in hormonal substances and other growth promoters
- (ff) illicit trafficking in nuclear or radioactive materials
- (gg) crimes falling within the jurisdiction of the International Criminal Court
- (hh) unlawful seizure of aircraft/ships, spacecraft
- (ii) sabotage

And, in addition, the following offences:

All other criminal offences which may give rise to extradition or surrender, to include also-

- (a) where compliant with national law, evading checks from law enforcement authorities; and
- (b) in relation to persons that can lead to the identification or the tracing of such suspected persons.

---

### **EXPLANATORY MEMORANDUM**

This Bill introduces legislation to provide law enforcement and other public authorities with investigatory powers such as interception of communication, acquisition of communications data, equipment interference, surveillance and decryption of protected information.

This Bill also provides oversight arrangements that strengthen the safeguards that apply to the use of such investigatory powers. The Bill places the key powers on a statutory footing and provides a structured, privacy-centred, proportionate and accountable framework. The legislation is supported by statutory codes of practice one for each of the key investigatory powers.

---

**Printed by the Gibraltar Chronicle Printing Limited  
Unit 3, New Harbours  
Government Printers for Gibraltar,  
Copies may be purchased at 6, Convent Place, Price. £8.00**