

**The Regulation of Investigatory Powers  
(Telecommunications) (Lawful Business Practice)  
(Interception of Communications) Regulations, 2004**

*Made*

*Coming into operation*

*14<sup>th</sup> June 2004*

*Laid before the States*

THE STATES HOME DEPARTMENT, in exercise of the powers conferred on it by sections 4(2) and 65 of the Regulation of Investigatory Powers (Bailiwick of Guernsey) Law, 2003<sup>1</sup> ("the Law"), hereby make the following Regulations: -

**Citation and commencement**

1. These Regulations may be cited as the Regulation of Investigatory Powers (Telecommunications) (Lawful Business Practice) (Interception of Communications) Regulations, 2004 and shall come into force on 14<sup>th</sup> June, 2004.

**Interpretation**

2. In these Regulations -

- (a) references to a business include references to activities of a government department, of any public authority or of any person or office holder on whom functions are conferred by or under any enactment;

---

<sup>1</sup> Order in Council No. XXX of 2003

- (b) a reference to a communication as relevant to a business is a reference to –
  - (i) a communication by means of which a transaction is entered into in the course of that business, or which otherwise relates to that business, or
  - (ii) a communication which otherwise takes place in the course of the carrying on of that business;
  
- (c) **“regulatory or self-regulatory practices or procedures”** means practices or procedures -
  - (i) compliance with which is required or recommended by, under or by virtue of any provision of the law, or under any standard or code of practice published by or on behalf of a body within the European Economic Area which includes amongst its objectives the publication of standards or codes of practice for the conduct of business, or
  - (ii) which are otherwise applied for the purpose of ensuring compliance with anything so required or recommended;
  
- (d) **“system controller”** means, in relation to a particular telecommunication system, a person with a right to control its operation or use.

**Lawful interception of a communication**

3. (1) For the purpose of section 1(5)(a) of the Law, and subject to paragraphs (3) and (4), conduct is authorised if it consists of interception of a

communication, in the course of its transmission by means of a telecommunication system, which is effected by or with the express or implied consent of the system controller for the purposes set out in paragraph (2).

(2) Those purposes are –

(a) monitoring or keeping a record of communications –

(i) in order to establish the existence of facts, or

(ii) to ascertain compliance with regulatory or self-regulatory practices or procedures which are applicable to the system controller in the carrying on of his business, or which are applicable to another person in the carrying on of his business where that person is supervised by the system controller in respect of those practices or procedures, or

(iii) to ascertain or demonstrate the standards which are achieved or ought to be achieved by persons using the system in the course of their duties, or

(iv) in the interests of national security, or

(v) for the purpose of preventing or detecting crime,  
or

(vi) for the purpose of investigating or detecting the unauthorised use of that or any other telecommunication system, or

(vii) where that is undertaken in order to secure, or as an inherent part of, the effective operation of the system (including any monitoring or keeping of a record which would be authorised by section 3(3) of the Law if the conditions in paragraphs (a) and (b) thereof are satisfied); or

(b) monitoring communications for the purpose of determining whether they are communications relevant to the system controller's business which fall within regulation 2(b)(i); or

(c) monitoring communications made to a confidential voice-telephony counselling or support service which is free of charge (other than the cost, if any, of making a telephone call) and operated in such a way that users may remain anonymous if they so choose.

(3) Conduct is authorised by paragraphs (1) and (2) of this regulation only if -

(a) the interception in question is effected solely for the purpose of monitoring or (where appropriate) keeping a record of communications relevant to the system controller's business

(b) the telecommunication system in question is provided for use wholly or partly in connection with that business;

(c) the system controller has made all reasonable efforts to inform every person who may use the telecommunication system in question that communications transmitted by means thereof may be intercepted; and

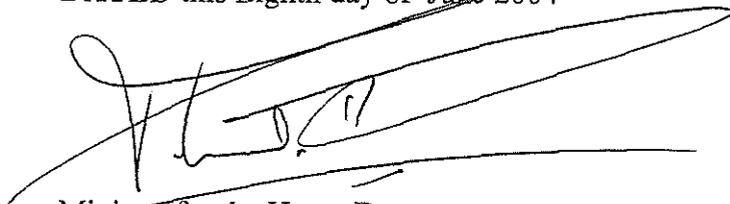
(d) in a case falling within -

(i) paragraph (2)(a)(iv), the person by or on whose behalf the interception is effected is a person specified in section 6(1)(a) to (e) of the Law;

(ii) paragraph (2)(b), the communication is one which is intended to be received (whether or not it has been actually received) by a person using the telecommunication system in question.

(4) Conduct falling within paragraph (2)(a)(i) to (iii) is authorised only to the extent that Article 5 of Directive 2002/58/EC of the European Parliament and of the Council of 12<sup>th</sup> July 2002 concerning the processing of personal data and the protection of privacy in the telecommunications sector so permits.

**DATED** this Eighth day of June 2004



Minister for the Home Department

For and on behalf of the Department

## EXPLANATORY NOTE

*(This note is not part of the Regulations)*

These Regulations authorise certain interceptions of telecommunication communications which would otherwise be prohibited by section 1 of the Regulation of Investigatory Powers (Bailiwick of Guernsey) Law, 2003. To the extent that the interceptions are also prohibited by Article 5.1 of Directive 2002/58/EC, the authorisation does not exceed that permitted by Articles 5.2 and 14.1 of the Directive.

The interception has to be by or with the consent of a person carrying on a business (which includes the activities of government departments, public authorities and others exercising statutory functions) for purposes relevant to that person's business and using that business's own telecommunication system.

Interceptions are authorised for specific business purposes only. These are -

- monitoring or recording communications:
  - to establish the existence of facts, to ascertain compliance with regulatory or self-regulatory practices or procedures or to ascertain or demonstrate standards which are or ought to be achieved (quality control and training),
  - in the interests of national security (in which case only certain specified public officials may make the interception),
  - to prevent or detect crime,
  - to investigate or detect unauthorised use of telecommunication systems or,

- to secure, or as an inherent part of, effective system operation;
- monitoring received communications to determine whether they are business or personal communications;
- monitoring communications made to anonymous telephone help-lines.

Interceptions are authorised only if the controller of the telecommunications system on which they are effected has made all reasonable efforts to inform potential users that interceptions may be made.

The Regulations do not authorise interceptions to which the persons making and receiving the communications have consented: these are not prohibited by the Law.