



# Government Gazette

**REPUBLIC OF SOUTH AFRICA**

**Vol. 470   Pretoria   4   August   2004   No. 26644**



**AIDS HELPLINE: 0800-0123-22 Prevention is the cure**

---

## GENERAL NOTICE

---

### NOTICE 1601 OF 2004 DEPARTMENT OF COMMUNICATIONS

**INVITATION TO INTERESTED PERSONS INCLUDING PRIVATE  
TELECOMMUNICATIONS NETWORK OPERATORS, WIRELESS DATA OPERATORS,  
MOBILE RADIO TRUNKING OPERATORS AND OTHER TELECOMMUNICATIONS  
OPERATORS EXCLUDING THE MOBILE CELLULAR OPERATORS, FIXED LINE  
OPERATOR OR INTERNET SERVICE PROVIDERS, TO SUBMIT WRITTEN  
COMMENTS ON THE DRAFT DIRECTIVE TO BE ISSUED IN TERMS OF THE  
REGULATION OF INTERCEPTION OF COMMUNICATIONS AND PROVISION OF  
COMMUNICATION-RELATED INFORMATION ACT, 2002**

The Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act No. 70 of 2002) (the Act) was assented to on the 22<sup>nd</sup> of January 2003.

The objectives of the Act amongst others are to regulate the –

- interception and monitoring of communications;
- making of applications for, and the issuing of directions authorizing the interception of communications and provision of communication-related information; and
- execution of directions and entry warrants by law enforcement officers.

Section 30 of the Act provides that all telecommunication service providers must provide a telecommunication service which has the capability to be intercepted and store communication-related information. The Minister of Communications is responsible for issuing directives to telecommunication service providers or categories of telecommunication service providers determining amongst others the –

- manner in which a telecommunication service provider must provide a service which is capable of being intercepted and store communication-related information;
- security, technical and functional requirements of the facilities and devices to be acquired by the telecommunication service providers to enable interception and storage;
- type of communication-related information which must be stored and the period for which such information must be stored; and
- period within which telecommunication service providers must comply with the directive.

A draft directive has been prepared that is available from the Department's website at [www.doc.gov.za](http://www.doc.gov.za)

Interested persons including Private Telecommunications Network Operators, Wireless Data Operators, Mobile Radio Trunking Operators and other Telecommunications Service Operators who have not been issued with the directive for Mobile Cellular Operators, Fixed line Operators or Internet Service Providers, are hereby invited to furnish comments on the directive no later than 16 August 2004 at any to the following addresses:

For Attention: Mr. E. Pitso / Mr. E. Baloyi  
Department of Communications

Post to: Private Bag X860  
Pretoria  
0001;

Or deliver to: First Floor, Block B  
iParioli Office Park  
399 Duncan Street  
Hatfield;

Or Fax to: (012) 427-8085

Or e-mail to: [elias@doc.gov.za](mailto:elias@doc.gov.za)  
[rina@doc.gov.za](mailto:rina@doc.gov.za)

Please note that comments received after the closing date may be disregarded

Mr. E. Pitso and Mr. E. Baloyi can be reached at tel.: (012) 427-8194 / 8100 / 8217 for any enquiries.

DRAFT DIRECTIVE FOR TELECOMMUNICATION  
SERVICE PROVIDERS WHO HAVE NOT BEEN  
ISSUED WITH THE DIRECTIVE FOR MOBILE  
CELLULAR OPERATORS, FIXED LINE  
OPERATORS OR INTERNET SERVICE  
PROVIDERS.

The Minister of Communications hereby-

- (a) in terms of section 30(7)(a) of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act No. 70 of 2002), read with section 30(2) of the said Act, issue the directive in the Schedule in respect of telecommunication service providers who have not been issued with the directive for mobile cellular operators, fixed line operators or internet service providers.
- (b) in terms of section 30(7)(b) of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act No. 70 of 2002), determine a period of six months for compliance by the said telecommunication service providers with the said directive.

## **SCHEDULE**

### **DIRECTIVE FOR TELECOMMUNICATION SERVICE PROVIDERS IN TERMS OF SECTION 30(7)(a) READ WITH SECTION 30(2) OF THE REGULATION OF INTERCEPTION OF COMMUNICATIONS AND PROVISION OF COMMUNICATION- RELATED INFORMATION ACT, 2002 (ACT NO. 70 OF 2002)**

#### **ARRANGEMENT OF CONTENT**

##### **PART 1: INTRODUCTORY PROVISIONS**

1. Definitions
2. Application
3. Statement of general duties

##### **PART 2: INTERCEPTION OF INDIRECT COMMUNICATIONS**

4. General requirements in respect of interception
5. Unchanged state of service
6. Security requirements for interception
7. Technical and functional requirements in respect of interception

##### **PART 3: PROVISION AND STORING OF REAL-TIME COMMUNICATION-RELATED INFORMATION**

8. General requirements in respect of real-time communication-related information
9. Provision and content of additional real-time communication-related information during active intercept or in respect of future information
10. Provision, recording, storing and content of real-time communication-related information already available
11. Security requirements in respect of real-time communication-related information
12. Technical and functional requirements in respect of real-time communication-related information

---

**PART 4: PROVISION AND STORING OF ARCHIVED  
COMMUNICATION-RELATED INFORMATION**

13. General requirements in respect of archived communication-related information
14. Content of archived communication-related information
15. Security requirements in respect of archived communication-related information
16. Technical and functional requirements in respect of archived communication-related information

**PART 5: STORAGE PERIOD FOR COMMUNICATION-  
RELATED INFORMATION**

17. Period for which communication-related information must be stored

## PART 1: INTRODUCTORY PROVISIONS

### 1. Definitions

In this directive, unless the context otherwise indicates, a word or expression to which a meaning has been assigned in the Act has the meaning so assigned, and-

"Act" means the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act No. 70 of 2002);

"buffer" means the temporary storing of real-time communication-related information and "buffered" has a similar meaning;

"direction" means a written or oral interception direction, real-time communication-related direction or archived communication-related direction, as the case may be;

"identity" means a technical label which may represent the origin or destination of any telecommunications traffic, as a rule clearly identified by a logical or virtual telecommunications identity number (such as a personal telephone number or subscriber number) assigned to a physical access;

"Interception Centre" means an interception centre established in terms of section 32 of the Act and is herein referred to as the "IC";

"interception measure" means a technical measure which facilitates the interception of telecommunications traffic pursuant to the Act;

"interception target" means the customer whose indirect communications are to be intercepted, or whose real-time communication-related information or archived communication-related information is to be provided by a TSP to an authorised person or the IC, pursuant to a direction or request;

"quality of service" means the quality specification of a telecommunications channel, system, virtual channel, computer-telecommunications session, etc. Quality of service may be measured, for example, in terms of signal-to-noise ratio, bit error rate, message throughput rate or call blocking probability.

“result of interception” means the content of an indirect communication which is provided by a TSP to an authorised person or the IC, pursuant to an interception directive or request;

“request” means a request in terms of section 7 of the Act;

“solution” means the facilities and devices to be acquired by a TSP in terms of section 30(2)(a)(ii) of the Act to enable interception of indirect communications;

“target identity” means the identity associated with a target service (see below) used by the interception target; and

“target service” means a telecommunications service associated with an interception target and usually specified in a direction or request.

## **2. Application**

This directive applies to and is binding on all TSPs that have been issued with a licence under Chapter 5 of the Telecommunications Act, 1996 (Act No. 103 of 1996), and who have not been issued with the directive for mobile cellular operators, fixed line operators or internet service providers.

## **3. General Duties**

3.1 A TSP must provide a telecommunications service -

- (a) which has the capability to be intercepted; and
- (b) store communication-related information,

in accordance with the provisions of the Act and this directive.

3.2 When a direction or request is presented to a TSP, that TSP shall comply with the provisions of that direction or request.

## **PART 2: INTERCEPTION OF INDIRECT COMMUNICATIONS**

### **4. General requirements in respect of interception**

A TSP must-

- (a) provide a telecommunication service in respect of which the signals of all indirect communications can be intercepted;



- (b) acquire a solution to enable the interception of all indirect communications on its telecommunication system;
- (c) make the necessary solution available to an authorised person to enable the interception of indirect communications pursuant to a direction or request;
- (d) make available the necessary assistance, to enable the authorised person to intercept indirect communications pursuant to a direction or request; and
- (e) make the necessary solution available as well as the necessary assistance, to enable the authorised person to effect the necessary connections in order to intercept indirect communications pursuant to a direction or request.

4.2 In accordance with a direction or request a TSP shall ensure that -

- (a) the entire content of an indirect communication associated with a target identity can be intercepted during the entire period; and
- (b) any content of an indirect communication associated with a target identity which is stored in a technical storage facilities or is retrieved from such storage facilities can be intercepted during the entire period.

4.3 The ability to intercept indirect communications shall be provided by a TSP in respect of all interception targets utilising its telecommunications system and in respect of all target services.

4.4 The configuration of a TSPs telecommunication system and the solution that is acquired for interception purposes must be able to intercept indirect communications in such a way that any indirect communication that does not fall within the scope of the direction or request can be excluded.

4.5 After a direction or a request has been presented, interception of the indirect communications shall proceed in accordance with that direction or request.

## **5. Unchanged state of service**

5.1 Interception shall be implemented and operated in such manner that no unauthorised person can detect any change from the unintercepted state.

5.2 Interception shall be implemented and operated in such manner that communicating parties shall not detect any change from the unintercepted state

5.3 The operating facilities and equipment relating to the target service shall not be altered as a result of any interception measure and the operating facilities of any other service shall not be altered as a result of any interception measure.

5.4 The quality of service of the target service shall not be altered as a result of any interception measure. The quality of service of any telecommunications service other than the target service shall not be altered as a result of any interception measure.

## **6. Security requirements for interception**

6.1 Information on the manner in which interception measures are implemented in a given telecommunication installation shall not be made available to unauthorised persons.

6.2 Information relating to target identities and target services to which interception is being applied shall not be made available to unauthorised persons.

6.3 A TSP shall agree confidentiality on the manner in which interception measures are implemented in a given telecommunication installation with the manufacturers of his technical installations for the implementation of interception measures.

6.4 The technical arrangements required within a telecommunication system and the application of the solution to allow implementation of the interception measures shall be realized with due care, particularly with respect to the following:

- (a) The need to protect information on which and how many target identities are or were subject to interception and the periods during which the interception measures were active.
- (b) The restriction to a minimum number of staff engaged in implementation and operation of the interception measure.
- (c) To ensure the clear delimitation of functions and responsibilities and the maintenance of third-party telecommunications privacy, interception shall be carried out in such a manner that it is only accessible to authorized personnel.
- (d) The results of interception shall only be made available to the authorised person.
- (e) In order to ensure the integrity of the solution, no access in whatever form to the solution shall be granted to unauthorized persons.
- (f) TSPs shall take all necessary measures to protect the solution against misuse.
- (g) In order to prevent or trace misuse of the solution, any activation or application of these solutions in relation to a given identity shall be fully recorded, including any activation or application caused by faulty or unauthorized use, and the records shall cover all or some of-
  - (i) the target identities of the target service or target services concerned;
  - (ii) the beginning and end of the activation or application of the interception measure;
  - (iii) the name, surname, identity number and any other information necessary to identify the authorised person;
  - (iv) the names, surnames, identity numbers and any other information necessary to identify the personnel that provided the necessary assistance during an interception measure and
  - (v) a reference to the direction or request.

6.5 The TSPs shall take reasonable steps to ensure that the records referred to in paragraph 6.4(g) are secure and only accessible to specific nominated staff.

## **7. Technical and functional requirements in respect of interception**

7.1 The configuration of a TSPs telecommunication system and the solution shall provide the results of interception for the entire duration of the interception period.

7.2 The configuration of a TSPs telecommunication system and the solution shall enable the provisioning of the result of interception.

7.3 A TSP must ensure that the solution can be implemented and connected to its telecommunication system and provide the interception of indirect communications on its telecommunication system pursuant to a direction or request.

7.4 The telecommunication system in conjunction with the solution shall ensure that all indirect communications on its telecommunication system can be intercepted and be able to provide the results of interception for the entire duration of the interception measure.

7.5 The telecommunication system and the solution shall ensure that the quality of service of the telecommunications traffic provided through the solution is not inferior to that offered to the target service for each particular communication.

7.6 The telecommunication system when used in conjunction with the solution shall be such that the result of interception provided through the solution must be in an industry standard format.

7.5 The correlation between the indirect communication and communication-related information shall be unique.

7.6 A TSP shall ensure that the configuration of the telecommunication system and the solution is such that it can implement and operate each interception measure with no or the minimum involvement of third parties.

7.7 Where a TSP makes use of any other telecommunication service provider's telecommunication system, both that TSP and

that other telecommunication service provider must co-operate in the provision of interception, if required.

7.8 A TSP must ensure that-

- (a) any telecommunication service provider involved in the provision of interception facilities is given no more information relating to operational activities than is strictly necessary to allow authorized target services to be intercepted; and
- (b) any telecommunication service provider involved in the co-operative provision of interception facilities is given no more information relating to operational activities than is strictly necessary to allow authorised target services to be intercepted.

7.9 Where the special properties of a given telecommunication service, and the justified requirements of the applicant, necessitate the use of various identifying characteristics for determination of the indirect communications to be intercepted, the TSP shall ensure that the indirect communications can be intercepted on the basis of these characteristics. Identifying characteristics include, but are not limited to, the telephone number or subscriber number.

7.10 In each case the characteristics shall be identifiable without unreasonable effort and shall be such that they allow clear identification of the interception target.

7.11 A TSP shall ensure that interception on the basis of more than one direction or request can be effected in respect of one and the same interception target. Multiple directions or requests may be applicable to a single interception target to allow monitoring by more than one applicant.

7.12 If multiple directions or requests are applicable, a TSP shall take reasonable precautions to safeguard the identities of the LEAs concerned and to ensure the confidentiality of the investigations.

7.13 Multiple directions or requests may require different information in respect of the same interception target.

7.14 The arrangements made in a telecommunication system for the technical implementation of interception measures shall be set up and configured so as to enable the identification and elimination, without undue delay, of bottlenecks and potential bottlenecks in a regional or functional part of that system when several interception measures are operated concurrently.

7.22 Supplementary to the provisions of paragraph 7.14, above, TSPs shall monitor their capacity in respect of simultaneous interceptions and shall be able to upgrade any regional or functional part of their telecommunication system within a reasonable period of time.

### **PART 3: PROVISION AND STORING OF REAL-TIME COMMUNICATION-RELATED INFORMATION**

#### **8. General requirements in respect of real-time communication-related information**

8.1 A TSP must provide a telecommunication service in respect of which all real-time communication-related information can be provided to an authorised person or the IC.

8.2 A TSP must ensure that real-time communication-related information can immediately, on receipt of a direction, be provided to authorised person or the IC..

8.3 After a direction has been presented, the provision of the real-time communication-related information shall proceed in accordance with that direction.

#### **9. Content of additional real-time communication-related information during active intercept or in respect of future information**

9.1 When both a real-time communication-related direction as well as an interception direction or request, in respect of the same target identity, are received a TSP shall be able to provide the real-time communication-related information in accordance with the direction concerned-

- (i) when a call setup is attempted and a call control session has been established with the controlling network element;
- (ii) when a call is established (call is answered);
- (iii) when no successful call is established (call is not answered).

9.2 In the circumstances set out in paragraph 9.1, above, a TSP shall be able to provide the following real-time communication-related information to the LEA or IC for calls originating from, and originating in the TSPs telecommunication system and terminating to, the target identity:

- (a) Called number (destination of an outgoing communication by the target identity).

- (b) Calling number (telephone number of originating party of a terminating communication to the target identity).
- (c) Date, time and duration of the communication.
- (d) Supplementary service or facility used in association with the call (three party conference, call diversion immediate, abbreviated dialling, voice mail, etc.).
- (e) Intermediate numbers where target identity establishes conference calls or calls to link through services.
- (f) Telephone or subscriber number of target identity.
- (g) Nature of the telecommunication (e.g. fax, voice, or data).
- (h) Forwarding call number.

## **10 Provision, recording, storing and content of real-time communication-related information already available**

10.1 A TSP shall record and store the real-time communication-related information set out in paragraph 10.3 whenever a call is established.

10.2 When a real-time communication-related direction, that requires information that is already available in the records of a TSP is received, that TSP shall be able to immediately provide the real-time communication-related information set out in paragraph 10.3 in accordance with the direction concerned.

10.3 For the purposes of paragraphs 10.1 and 10.2, above, a TSP shall be able to provide the following real-time communication-related information for calls originating from, and originating in the TSP telecommunication system and terminating to, the target identity:

- (a) Called number (destination of an outgoing communication by the target identity).
- (b) Calling number (telephone number of originating party of a terminating communication to the target identity).
- (c) Date, time and duration of the communication.
- (d) Supplementary service or facility used in association with the call (three party conference, call diversion immediate, abbreviated dialling, voice mail, etc.).
- (e) Intermediate numbers where target identity establishes conference calls or calls to link through services.



- (f) Telephone or subscriber number of target identity.
- (g) Nature of the telecommunication (e.g. fax, voice, or data).
- (h) Forwarding call number.

10.4 A TSP must provide a telecommunication service in respect of which all real-time communication-related information set out in paragraph 10.3 can be securely stored, retrieved and duplicated for provision to a LEA or IC.

10.5 Real-time communication-related information set out in paragraph 10.3 must be immediately available in the records of the TSP for a period of at least 90 days from the date of the indirect communication to which the real-time communication-related information relates.

10.6 The real-time communication-related information set out in paragraph 10.3 must immediately be retrievable from the records of the TSP.

10.7 A TSP must ensure that real-time communication-related information set out in paragraph 10.3 can immediately, on receipt of a direction, be provided to the LEA or IC.

10.8 The real-time communication-related information set out in paragraph 10.3 must be stored in a format that allows for the extraction of the relevant requested information only, in a readable, intelligible and understandable format, and in accordance with the direction.

10.9 When the real-time communication-related information set out in paragraph 10.3 is transferred to an archived storage facility, the TSP must ensure that-

- (a) all the information set out in paragraph 14 is transferred;
- (b) the information is not transferred before the expiry of 90 days from the date on which the indirect communication to which the real-time communication-related information relates, is recorded; and
- (c) the integrity of the information is not compromised.

## **11. Security requirements in respect of real-time communication-related information**

11.1 Information on the manner in which storage measures in respect of real-time communication-related information are implemented by a TSP shall not be made available to unauthorized persons.

11.2 Real-time communication-related information shall not be made available to unauthorized persons.

11.3 The TSP shall agree confidentiality on the manner in which storage measures in respect of real-time communication-related information are implemented with the manufacturers of his technical installations for the implementation of storage measures.

11.4 The technical arrangements required within a TSP, to allow implementation of the storage measures in respect of real-time communication-related information, shall be realized with due care exercised in operating telecommunication installations, particularly with respect to the following:

- (a) The need to protect information on which and how many target identities are or were subject to a real-time communication-related direction and the periods in respect of which the directions were applicable.
- (b) The restriction to a minimum of staff engaged in implementation and operation of storing measures in respect of real-time communication-related information.
- (c) To ensure the clear delimitation of functions and responsibilities and the maintenance of third-party telecommunications privacy, storing facilities in respect of real-time communication-related information shall be accessible only by authorized personnel.
- (d) Real-time communication-related information shall be provided to a LEA or IC.
- (e) Authentication and proof of authentication shall be implemented subject to national laws and regulations and as agreed upon by the IC and TSP.
- (f) In order to prevent or trace misuse of the technical functions integrated in the telecommunication installation enabling the storing and provision of real-time communication-related information, any activation or application of these functions in relation to a given

identity shall be fully recorded, including any activation or application caused by faulty or unauthorized input, and the records shall cover all or some of-

- (i) the target identities of the target service or target services concerned;
- (ii) the beginning and end of the activation or application of the real-time communication-related direction;
- (iii) the IC to which the real-time communication-related information is routed or LEA to which it is provided;
- (iv) an authenticator suitable to identify the operating staff (including date and time of input); and
- (v) a reference to the direction.

11.5 The TSP shall take reasonable steps to ensure that the records referred to in paragraph 11.4(f) are secure and only accessible to specific nominated staff.

11.6 The TSP shall take reasonable steps to ensure the integrity of real-time communication-related information when it is recorded and stored.

11.7 A TSP shall take reasonable steps to ensure the physical, environmental and logical security of all stored real-time communication-related information.

11.8 A TSP shall employ reasonable measures to ensure the availability of real-time communication-related information.

## **12. Technical and functional requirements in respect of real-time communication-related information**

12.1 The technical handover interface or solution shall provide all the relevant requested real-time communication-related information only, in a readable, intelligible and understandable format, and in accordance with the direction.

12.2 The configuration of the handover interface or solution shall be such that the provision of the requested real-time communication-related information can be implemented with standard, generally available protocols and coding principles.

12.3 The format for providing the requested real-time communication-related information to the LEA or IC must be an industry standard format.

12.4 The IC must be informed of-

- (a) any change of the storage system, measures and functionality that may impact on the provision or configuration of real-time communication-related information; and
- (b) the temporary unavailability of stored real-time communication-related information.

12.5 A TSP shall ensure that the configuration of the storage system is such that it can store, maintain, extract, process or provide real-time communication-related information with no or the minimum involvement of third parties.

12.6 Where a TSP makes use of any telecommunication service provider's telecommunication system or storage provider's service, that TSP and other telecommunication service provider or storage provider must co-operate in the storing or provision of real-time communication-related information, if required.

12.9 A TSP must ensure that-

- (a) any telecommunication service provider or storage provider involved in the storing and provision of real-time communication-related information is given no more information relating to operational activities than is strictly necessary to store and provide real-time communication-related information; and
- (b) any telecommunication service provider or storage provider involved in the co-operative storing and provision of real-time communication-related information is given no more information relating to operational activities than is strictly necessary to allow the storing and provisioning of real-time communication-related information.

12.10 When the provision of all the requested real-time communication-related information is, in exceptional cases, not

possible the remainder of the real-time communication-related information shall nevertheless be provided to the LEA or IC.

12.11 Storage devices or media shall be clearly indexed or the information contained identified to ensure the retrieval of only requested real-time communication information without unreasonable effort or delay.

12.12 The TSP shall ensure that more than one direction for real-time communication-related information can be operated concurrently for one and the same storage device or media.

12.13 If one or more direction for real-time communication-related information is processed, TSPs shall take reasonable precautions to safeguard the identities of the LEAs and ensure the confidentiality of the investigations and information.

## **PART 4: PROVISION AND STORING OF ARCHIVED COMMUNICATION-RELATED INFORMATION**

### **13. General requirements in respect of archived communication-related information**

13.1 A TSP must provide a telecommunication service in respect of which all archived communication-related information can be securely stored, retrieved and duplicated for provision to a LEA or IC.

13.2 Archived communication-related information must be available in the storage facility of the TSP for the period specified in paragraph 17.

13.3 Archived communication-related information must be retrievable from the storage facility of the TSP.

13.4 A TSP must ensure that archived communication-related information can within the period specified in the direction, be provided to the LEA or IC.

13.5 Archived communication-related information must be stored in a format that allows for the extraction of the relevant requested information only, in a readable, intelligible and understandable format, and in accordance with the direction.

13.6 If real-time communication-related information is transferred to an archived storage facility, the TSP must ensure that-

- (a) all the information set out in paragraph 14 is transferred;
- (b) the information is not transferred before the expiry of 90 days from the date on which the indirect communication to which the real-time communication-related information relates, is recorded; and
- (c) the integrity of the information is not compromised.

13.7 After a direction has been presented, the provision of the archived communication-related information shall proceed in accordance with that direction.

**14. Content of archived communication-related information**

TSPs shall store and be able to provide the following archived communication-related information:

- (a) Called telephone number or address (destination of outgoing communication by the target identity).
- (b) Date, time and duration of the communication.
- (c) Supplementary service or facility used in association with the call (three party conference, call diversion immediate, abbreviated dialling, voice mail, etc.).
- (d) Telephone number of target identity.
- (e) Forwarding call number.

**15. Security requirements in respect of archived communication-related information**

15.1 Information on the manner in which storage measures in respect of archived communication-related information are implemented by a TSP shall not be made available to unauthorized persons.

15.2 Archived communication-related information shall not be made available to unauthorized persons.

15.3 The TSP shall agree confidentiality on the manner in which storage measures in respect of archived communication-related information are implemented with the manufacturers of his technical installations for the implementation of storage measures.

15.4 The technical arrangements required within a TSP, to allow implementation of the storage measures in respect of archived communication-related information, shall be realized with due care exercised in operating telecommunication installations, particularly with respect to the following:

- (a) The need to protect information on which and how many target identities are or were subject to a archived communication-related direction and the periods in respect of which the directions were applicable.
- (b) The restriction to a minimum of staff engaged in implementation and operation of storing measures in respect of archived communication-related information.
- (c) To ensure the clear delimitation of functions and responsibilities and the maintenance of third-party

telecommunications privacy, storing facilities in respect of archived communication-related information shall be accessible only by authorized personnel.

- (d) Archived communication-related information shall be provided to a LEA or IC.
- (e) In order to prevent or trace misuse of the technical functions integrated in the telecommunication installation enabling the storing and provision of archived communication-related information, any activation or application of these functions in relation to a given identity shall be fully recorded, including any activation or application caused by faulty or unauthorized input, and the records shall cover all or some of-
  - (i) the target identities of the target service or target services concerned;
  - (ii) the beginning and end of the activation or application of the archived communication-related direction;
  - (iii) the IC to which the real-time communication-related information is routed or LEA to which it is provided;
  - (iv) an authenticator suitable to identify the operating staff (including date and time of input); and
  - (v) a reference to the direction.

15.5 The TSPs shall take reasonable steps to ensure that the records referred to in paragraph 15.4(e) are secure and only accessible to specific nominated staff.

15.6 The TSP shall take reasonable steps to ensure the integrity of archived communication-related information when it is stored, during transfer thereof to any storage device or media and for the entire storage period set out in paragraph 17.

15.7 A TSP shall take reasonable steps to ensure the physical, environmental and logical security of all stored archived communication-related information.

15.8 A TSP shall employ reasonable measures to ensure the availability of archived communication-related information.



## **16. Technical and functional requirements in respect of archived communication-related information**

16.1 The technical handover interface shall provide all the relevant requested archived communication-related information only, in a readable, intelligible and understandable format, and in accordance with the direction.

16.2 The configuration of the handover interface shall be such that the provision of the requested archived communication-related information provided at the interface can be implemented with industry standard, generally available protocols and coding principles.

16.3 The format for providing the requested archived communication-related information to the LEA or IC must be an industry standard format.

16.4 The IC must be informed of-

- (a) any change of the storage system, measures and functionality that may impact on the provision or configuration of archived communication-related information ; and
- (b) the temporary unavailability of stored archived communication-related information.

16.5 A TSP shall ensure that the configuration of the storage system is such that it can store, maintain, extract, process and provide archived communication-related information with no or the minimum involvement of third parties.

16.6 Where a TSP makes use of any telecommunication service provider's telecommunication system or storage provider's service, that TSP and other telecommunication service provider or storage provider must co-operate in the storing and provision of archived communication-related information, if required.

16.7 A TSP must ensure that-

- (a) any telecommunication service provider or storage provider involved in the storing and provision of archived communication-related information is given no more information relating to operational activities than

- is strictly necessary to store and provide archived communication-related information; and
- (b) any telecommunication service provider or storage provider involved in the co-operative storing and provision of archived communication-related information is given no more information relating to operational activities than is strictly necessary to allow the storing and provisioning of archived communication-related information.

16.8 When the provision of all the requested archived communication-related information is, in exceptional cases, not possible the remainder of the archived communication-related information shall nevertheless be provided to the LEA or IC.

16.9 Storage devices or media shall be clearly indexed or the information contained identified to ensure the retrieval of only requested archived communication-related information without unreasonable effort or delay.

16.10 The TSP shall ensure that more than one direction for archived communication-related information can be operated concurrently for one and the same storage device or media.

16.11 If one or more direction for archived communication-related information are processed, TSPs shall take reasonable precautions to safeguard the identities of the LEAs and ensure the confidentiality of the investigations and information.

## **PART 5: STORAGE PERIOD FOR COMMUNICATION-RELATED INFORMATION**

### **17. Period for which communication-related information must be stored**

Communication-related information, whether real-time or archived communication-related information, must be stored for a cumulative period of 3 years from the date on which the indirect communication to which the communication-related information relates, is recorded.

---