

RECOMMENDATION NO.R (95) 4 AND EXPLANATORY MEMORANDUM

OF THE PROTECTION OF PERSONAL DATA IN THE AREA OF TELECOMMUNICATION SERVICES, WITH PARTICULAR REFERENCE TO TELEPHONE SERVICES

*(adopted by the Committee of Ministers on 7 February 1995 at the 528th meeting of the
Ministers' Deputies)*

Preamble

The Committee of Ministers, under the terms of Article 15.b of the Statute of the Council of Europe,

Considering that the aim of the Council of Europe is to achieve a greater unity among its members;

Aware of the increasing use of automated data processing in the area of telecommunication services, as well as the advantages to be gained by users from technological developments, in particular in the area of telephone services;

Bearing in mind in this regard the move towards digitalisation of networks, with the advantages which this brings to users of telecommunication services;

Believing, nevertheless, that technological development in the area of telecommunications, in particular telephone services, may entail possible risks to the privacy of the user, as well as possible inhibitions on his freedom of communication;

Referring, in this regard, to certain new features particularly in the area of telephone services, for instance, calling-line identification, call-forwarding and mobile telephones, as well as malicious call-tracing devices and automatic-dialling devices;

Noting also the risks to privacy and freedom of communication accompanying the provision of itemised telephone bills;

Recognising that the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Strasbourg 1981; ETS No. 108) apply to the automated data processing activities of network operators and other parties providing telecommunication services;

Believing, however, that it is appropriate to apply more specifically the general provisions of the convention so as to adapt them to the collection and processing of personal data by network operators and any other party providing telecommunication services;

Noting, in addition, that new developments in telecommunication services must respect the right to private life and secrecy of correspondence as guaranteed by Article 8 of the European Convention on Human Rights,

Recommends that the governments of member states:

- take account in their domestic law and practice of the principles annexed to this recommendation;
- bring this recommendation to the attention of any authority involved in the implementation of national policies in respect of data protection or telecommunications;
- ensure that the provisions of the recommendation are brought to the attention of network operators, providers of telecommunication services, equipment and software suppliers, organisations using telecommunications means for direct marketing, as well as bodies representing any of these and consumer organisations;
- promote the provisions of the recommendation within the various international bodies dealing with telecommunications.

Appendix to Recommendation No. R (95) 4

1. Scope and definitions

- 1.1. The principles contained in this recommendation apply to network operators and service providers who for the accomplishment of their functions collect and process personal data.
- 1.2. These principles apply to personal data undergoing automatic processing. Member states may extend the principles contained in this recommendation to personal data undergoing manual processing.
- 1.3. Member states may extend the principles contained in this recommendation to the collection and processing of personal data relating to legal persons.
- 1.4. For the purposes of this recommendation:
 - the term "personal data" covers any information relating to an identified or identifiable individual (data subject). An individual shall not be regarded as "identifiable" if identification requires an unreasonable amount of time or manpower;
 - the term "telecommunication services" covers the various services offered over telecommunication networks for voice, text, image and data transmission between users in communication or correspondence;
 - the term "network operators" refers to any public or private entity which makes available the use of telecommunication networks;
 - the term "service providers" refers to any public or private entity which provides and operates telecommunication services using a network made available by a network operator or using its own network.

2. Respect for privacy

- 2.1. Telecommunication services, and in particular telephone services which are being developed, should be offered with due respect for the privacy of users, the secrecy of correspondence and the freedom of communication.

- 2.2. Network operators, service providers and equipment and software suppliers should exploit information technology for constructing and operating networks, equipment and software, in a way which ensures the privacy of users.

Anonymous means of accessing the telecommunication network and services should be made available.

- 2.3. Unless authorised for technical storage or message transmission or for other legitimate purposes, or for the execution of a service contract with the subscriber, any interference by network operators or service providers with the content of communications should be prohibited. Subject to Principle 4.2, the data pertaining to the content of messages collected during any such interference should not be communicated to third parties.

- 2.4. Interference by public authorities with the content of a communication, including the use of listening or tapping devices or other means of surveillance or interception of communications, must be carried out only when this is provided for by law and constitutes a necessary measure in a democratic society in the interests of:

- a) protecting state security, public safety, the monetary interests of the state or the suppression of criminal offences;
- b) protecting the data subject or the rights and freedoms of others.

- 2.5. In the case of interference by public authorities with the content of a communication, domestic law should regulate:

- a) the exercise of the data subject's rights of access and rectification;
- b) in what circumstances the responsible public authorities are entitled to refuse to provide information to the person concerned, or delay providing it;
- c) storage or destruction of such data.

If a network operator or service provider is instructed by a public authority to effect an interference, the data so collected should be communicated only to the body designated in the authorisation for that interference.

- 2.6. Domestic law should determine the conditions and safeguards under which network operators are authorised to use technical means to locate the source of malicious or abusive calls.

3. Collection and processing of data

- 3.1. The collection and processing of personal data in the area of telecommunication services should take place and develop within the framework of data protection policy, taking account of the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and in particular the principle of purpose specification.

Without prejudice to other purposes foreseen in this recommendation, personal data should only be collected and processed by network operators and service providers for the purposes of connecting a user to the network and making available to him a particular telecommunication service and for billing and verification purposes, as well as for ensuring the optimal technical operation and development of the network and service.

- 3.2. Network operators and service providers should inform, in an appropriate manner, subscribers to the various telecommunication services of the categories of personal data concerning them which they collect and process, the legal bases of collection, the purposes

for which they are collected and processed, the use made of the data and the periods over which they are stored.

4. Communication of data

- 4.1. Personal data collected and processed by network operators or service providers should not be communicated, unless the subscriber concerned has given in writing his express and informed consent and the information communicated does not make it possible to identify called parties.

The subscriber may revoke his consent at any time but without retroactive effect.

- 4.2. Personal data collected and processed by network operators or service providers may be communicated to public authorities when this is provided for by law and constitutes a necessary measure in a democratic society in the interests of:

- a) protecting state security, public safety, the monetary interests of the state or the suppression of criminal offences;
- b) protecting the data subject or the rights and freedoms of others.

- 4.3. In cases of communication to public authorities of personal data, domestic law should regulate:

- a) the exercise of rights of access and rectification by the data subject;
- b) the conditions under which the competent public authorities shall be entitled to refuse to give information to the data subject or to defer the issue thereof;
- c) conservation or destruction of such data.

- 4.4. Subscriber lists which contain personal data may only be communicated by network operators and service providers to third parties if one of the following conditions has been met:

- a) the subscriber has given in writing his express and informed consent; or
- b) the subscriber has been informed of the intended communication and has not objected; or
- c) the data protection authority has authorised the communication; or
- d) communication is provided for under domestic law.

The subscriber may revoke his consent at any time but without retroactive effect.

- 4.5. Communication of personal data between network operators and service providers is allowed where such communication is necessary for operational and invoicing purposes.

5. Rights of access and rectification

- 5.1. Each subscriber should, on request and at reasonable intervals and without excessive delay or expense, be able to obtain all data concerning him which have been collected and processed by network operators or service providers, and to have them rectified or erased where they are found to be inaccurate, irrelevant or excessive, or where they have been stored for an excessive length of time.

- 5.2. Fulfilment of the requests made under Principle 5.1 may be refused, limited or postponed when this is provided for by law and constitutes a necessary measure in a democratic society in the interests of:

- a) protecting state security, public safety, the monetary interests of the state or the suppression of criminal offences;
- b) protecting the data subject or the rights and freedoms of others.

6. Security

- 6.1. Network operators and service providers should take all appropriate technical and organisational measures to ensure the physical and logical security of the network, services and the data which they collect and process, and to prevent unauthorised interference with, or interception of, communications.
- 6.2. Subscribers to telecommunications services should be informed about network security risks and methods for subscribers to reduce the security risks of their messages.

7. Implementation of principles

a. Directories

- 7.1. Subscribers should have the right to refuse without justification and at no extra cost, to have their personal data included in a directory.

Where domestic law requires certain data to be included in a directory, however, the subscriber should be entitled to have his data excluded for valid reasons.

Where domestic law requires a subscriber to pay a fee for ex-directory facilities, any such fee should not exceed a reasonable amount and should in no case be a deterrent to exercising the right to take advantage of ex-directory facilities.

- 7.2. A subscriber wishing to have data concerning co-users of his terminal included in a directory should first obtain the consent of the latter.
- 7.3. Subject to the wish of the subscriber to have additional data concerning himself included, the personal data contained in a directory should be limited to such as are necessary to identify reasonably a particular subscriber and to avoid confusion between or among different subscribers listed in the directory.
- 7.4. When an electronic directory is consulted, technical means should be provided to prevent abuse and in particular unauthorised remote downloading.

The matching of data contained in an electronic directory with other data or files should be prohibited unless this is allowed by domestic law or is essential to the network operators or service providers for operational purposes.

- 7.5. Data contained in a directory may be used by network operators or service providers to operate a service replying to precise enquiries about the directory. Answers to directory enquiries should be limited to communication of the data appearing in the directory. Measures should be taken to prevent abuse. Directory enquiries services should not provide information relating to subscribers not appearing in the directory except with their written and informed consent.
- 7.6. Use of data appearing in the directory shall also be governed by the relevant principles of Recommendation No. R (91) 10 on the communication to third parties of personal data held by public bodies.

b. Use of data for the purposes of direct marketing

- 7.7. The principles laid down in Recommendation No. R (85) 20 on the protection of personal data used for the purposes of direct marketing apply to the use of subscriber data by third parties for purposes of direct marketing.
- 7.8. Domestic law should provide the appropriate guarantees and determine the conditions under which subscriber data may be used by network operators, service providers and third parties for the purposes of direct marketing by telephone or by other telecommunication means.
- 7.9. The elaboration of codes of practice should be encouraged so as to ensure that the practice is carried out in a way which does not cause distress or discomfort to subscribers. In particular, domestic law or codes of practice should apply to the time when calls may be made, the nature of the message and the manner in which the message is communicated.
- 7.10. Direct marketing by telephone or by other telecommunication means may not be directed at any subscriber who has expressed the wish not to receive any advertising material. For this purpose, appropriate means should be developed for identifying those subscribers who do not wish to receive any advertising material over the telephone.
- 7.11. Automatic call devices for transmitting pre-recorded messages of an advertising nature, may only be directed at subscribers who have given their express and informed consent to providers of this sort of service. The subscriber may revoke his consent at any time.

c. Detailed billing

- 7.12. Itemised bills should only be made available by network operators and service providers to the subscriber on his request. Consideration should be given to the privacy of the co-users and correspondents.
- 7.13. Data needed for billing should not be stored by network operators or service providers for a period which is longer than strictly necessary for settling the account, bearing in mind the possible need to store data for a reasonable period with a view to complaints on the billing, or if legal provisions require those data to be kept longer.

d. Private branch exchange systems (PBX systems)

- 7.14. In principle, individuals should be informed by appropriate means whenever data resulting from the use of a telephone are collected and processed by the operator of the private branch exchange. The data stored should be erased immediately on payment of the invoice.
- 7.15. The principles laid down in Recommendation No. R (89) 2 on the protection of personal data used for employment purposes apply to the operation by employers of telephone call logging systems at their places of work.

e. Calling-line identification

- 7.16. The introduction of a service feature permitting the display of the telephone number of an incoming call on the called subscriber's terminal should be accompanied by information to all subscribers that this feature is now available to some subscribers, and therefore that the possibility exists that their telephone number may be disclosed to the called subscriber.

The introduction of this feature should be accompanied by the possibility of the calling party to prevent in a simple manner the disclosure of their telephone number to the called party.

- 7.17. Domestic law should determine the conditions and safeguards under which network operators are authorised or obliged to override the decision of a calling party to suppress the display of his number on the called party's terminal.

f. Call forwarding

- 7.18. Consideration should be given to mechanisms whereby a third party subscriber may seek cancellation of call forwarding in case of dispute.
- 7.19. Where, in accordance with the provisions of Principle 2.4 relating to interception of communications, the surveillance or interception of incoming and outgoing calls of a subscriber has been authorised, the surveillance or interception measures should not extend to all incoming calls on the terminal of a third party subscriber but only to those which have been forwarded by the former.

g. Mobile telephones

- 7.20. When providing and operating a mobile telephone service, network operators and service providers should inform subscribers of the risks for secrecy of correspondence which may accompany the use of mobile telephone networks, in particular in the absence of encryption of radiocommunications. Means of offering encryption possibilities or equivalent safeguards to subscribers to mobile telephone networks should be found.
- 7.21. Consideration should be given to the need to ensure that billing for the use of a mobile telephone does not require the storage of data revealing with too great a precision the location of the subscriber or the called party at the time of use.