COUNCIL OF EUROPE
COMMITTEE OF MINISTERS

RECOMMENDATION No. R (99) 5

OF THE COMMITTEE OF MINISTERS TO MEMBER STATES

FOR THE PROTECTION OF PRIVACY ON THE INTERNET

(Adopted by the Committee of Ministers on 23 February 1999 at the 660th meeting of the Ministers' Deputies)

GUIDELINES
for the protection of individuals with regard to the collection and processing of personal data on information highways

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 greater unity among its members;

Noting the developments in new technologies and new communications and on-line information services;

Aware that these developments will influence the functioning of society in general and relations between individuals, in particular in offering increased possibilities for communication and exchange of information at national and international levels;

Aware of the advantages which users of new technologies can gain from these developments;

Considering, nevertheless, that technological development and the generalisation of collection and processing of personal data on information highways carries risks for the privacy of natural persons;

Considering that technological development also makes it possible to contribute towards the respect of fundamental rights and freedoms, and in particular the right to privacy, when personal data concerning natural persons are processed;

Aware of the need to develop techniques which permit the anonymity of data subjects and the confidentiality of the information exchanged on information highways while respecting the rights and freedoms of others and the values of a democratic society;

Aware that communications carried out with the aid of new information technologies must also respect the human rights and fundamental freedoms and, in particular, the right to privacy and to secrecy of correspondence, as guaranteed by Article 8 of the European Convention on Human Rights;

Recognising that the collection, processing and especially communication of personal data by means of new information technologies, particularly the information highways, are governed by the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Strasbourg 1981, European Treaty Series No. 108) and by sectoral recommendations on data protection and notably Recommendation No. R (90) 19 on the protection of personal data used for payment and other related operations, Recommendation No. R (91) 10 on the communication to third parties of personal data held by public bodies, and Recommendation No. R (95) 4 on the protection of personal data in the area of telecommunications, with particular reference to telephone services;

Considering that it is appropriate to make users and Internet service providers aware of the general provisions of the above-mentioned convention with regard to the collection and processing of personal data on information highways;

Recommends that the governments of member States disseminate widely the Guidelines contained in the appendix to this recommendation, especially to users and service providers on the Internet as well as to any national authority responsible for supervising respect of data protection provisions.

Appendix to Recommendation No. R (99) 5

Guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways which may be incorporated in or annexed to codes of conduct

I. Introduction

These guidelines set out principles of fair privacy practice for users and Internet service providers (ISP).[1] These principles may be taken up in codes of conduct.

Users should be aware of the responsibilities of ISPs and vice versa. Therefore it is advisable that users and ISPs read the whole text, although for ease of use it is divided into several parts. You may be concerned by one or more parts of the guidelines.

Use of the Internet places responsibilities on each of your actions and poses risks to privacy. It is important to behave in a way that provides protection to yourself and promotes good relations with others. These guidelines suggest some practical ways to safeguard privacy, but you should also know your legal rights and obligations.

Remember that respect for privacy is a fundamental right of each individual which may also be protected by data protection legislation. So it may be well worth checking your legal position.

II. For Users

1. Remember that the Internet is not secure. However, different means exist and are being developed enabling you to improve the protection of your data[2]. Therefore, use all available

[1] See part IV, paragraph 1.

[2] The word "data" refers to "personal data" which concern you or other people.

means to protect your data and communications, such as legally available encryption for confidential e-mail, as well as access codes to your own personal computer.[3]

2. Remember that every transaction you make, every site you visit on the Internet leaves traces. These "electronic tracks" can be used, without your knowledge, to build a profile of what sort of person you are and your interests. If you do not wish to be profiled, you are encouraged to use the latest technical means which include the possibility of being informed every time you leave traces, and to reject such traces. You may also ask for information about the privacy policy of different programmes and sites and give preference to those which record few data or which can be accessed in an anonymous way.

3. Anonymous access to and use of services, and anonymous means of making payments, are the best protection of privacy. Find out about technical means to achieve anonymity, where appropriate.[4]

4. Complete anonymity may not be appropriate because of legal constraints. In those cases, if it is permitted by law, you may use a pseudonym so that your personal identity is known only to your ISP.

5. Only give your ISP, or any other person, such data as are necessary in order to fulfil a specific purpose you have been informed about. Be especially careful with credit card and account numbers, which can be used and abused very easily in the context of the Internet.

6. Remember that your e-mail address is personal data, and that others may wish to use it for different purposes, such as inclusion in directories or user lists. Do not hesitate to ask about the purpose of the directory or other use. You can request to be omitted if you do not want to be listed.

7. Be wary of sites which request more data than are necessary for accessing the site or for making a transaction, or which do not tell you why they want all these data from you.

8. Remember that you are legally responsible for the processing of data, for example, if you illicitly upload or download, and that everything may be traced back to you even if you use a pseudonym.

9. Do not send malicious mail. It can bounce back with legal consequences.

10. Your ISP is responsible for proper use of data. Ask your ISP what data he/she collects, processes and stores, in what way and for what purpose. Repeat this request from time to time. Insist that your ISP change them if they are wrong or delete them if they are excessive, out of date or no longer required. Ask the ISP to notify this modification to other parties to whom he or she has communicated your data. [5]

11. If you are not satisfied with the way your current ISP collects, uses, stores or communicates data, and he or she refuses to change his or her ways, then consider moving to another ISP. If you believe that your ISP does not comply with data protection rules, you can inform the competent authorities or take legal action.

---

[3] For example, use passwords and change them regularly.

[4] For example by using public Internet kiosks or pre-paid access and payment cards.

[5] Data protection laws, following Article 5 of the Council of Europe Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), give responsibility for the accuracy and up-dating of data to the person who processes them.

12. Keep yourself informed of the privacy and security risks on the Internet as well as the methods available to reduce such risks.

13. If you intend to send data to another country, you should be aware that data may be less well protected there. If data about you are involved, you are free, of course, to communicate these data nevertheless. However, before you send data about others to another country, you should seek advice, for example from the authority of your country, on whether the transfer is permissible.[6] You might have to ask the recipient to provide safeguards[7] necessary to ensure protection of the data.

III. For Internet service providers

1. Use appropriate procedures and available technologies, preferably those which have been certified, to protect the privacy of the people concerned (even if they are not users of the Internet), especially by ensuring data integrity and confidentiality as well as physical and logical security of the network and of the services provided over the network.

2. Inform users of privacy risks presented by use of the Internet before they subscribe or start using services. Such risks may concern data integrity, confidentiality, the security of the network or other risks to privacy such as the hidden collection or recording of data.

3. Inform users about technical means which they may lawfully use to reduce security risks to data and communications, such as legally available encryption and digital signatures. Offer such technical means at a cost-oriented price, not a deterrent price.

4. Before accepting subscriptions and connecting users to the Internet, inform them about the possibilities of accessing the Internet anonymously, and using its services and paying for them in an anonymous way (for example, pre-paid access cards). Complete anonymity may not be appropriate because of legal constraints. In those cases, if it is permitted by law, offer the possibility of using pseudonyms. Inform users of programmes allowing them to search and browse anonymously on the Internet. Design your system in a way that avoids or minimises the use of personal data.

5. Do not read, modify or delete messages sent to others.

6. Do not allow any interference with the contents of communications, unless this interference is provided for by law and is carried out by a public authority.

7. Collect, process and store data about users only when necessary for explicit, specified and legitimate purposes.

8. Do not communicate data unless the communication is provided for by law.[8]

---

[6] The laws of numerous European countries forbid transfers to countries which do not ensure an adequate or equivalent level of protection to that of your country. Exceptions are nevertheless provided for, in particular if the person concerned has consented to the transfer of his or her data to such countries.

[7] These safeguards may be developed and/or presented in particular in a contract on transborder data flows.

[8] In general, data protection laws permit communication to third parties under certain conditions, in particular:

9. Do not store data for longer than is necessary to achieve the purpose of processing.[9]

10. Do not use data for your own promotional or marketing purposes unless the person concerned, after having been informed, has not objected or, in the case of processing of traffic data or sensitive data, he or she has given his or her explicit consent.

11. You are responsible for proper use of data. On your introductory page highlight a clear statement about your privacy policy. This statement should be hyperlinked to a detailed explanation of your privacy practice. Before the user starts using services, when he or she visits your site, and whenever he or she asks, tell him or her who you are, what data you collect, process and store, in what way, for what purpose and for how long you keep them. If necessary, ask for his or her consent. At the request of the person concerned, correct inaccurate data immediately and delete them if they are excessive, out of date or no longer required and stop the processing carried out if the user objects to it. Notify the third parties to whom you have communicated the data of any modification. Avoid the hidden collection of data.

12. Information provided to the user must be accurate and kept up to date.

13. Think twice about publishing data on your site! Such publication may infringe other people's privacy and may also be prohibited by law.

14. Before you send data to another country seek advice, for example from the competent authorities in your country, on whether the transfer is permissible.[10] You may have to ask the recipient to provide safeguards necessary to ensure protection of the data.[11]

IV. Clarification and remedies

1. Where in this text the term ISP is used, the same applies, where appropriate, to other actors on the Internet, such as access providers, content providers, network providers, navigation software designers, bulletin board operators, and so on.

2. It is important to ensure that your rights are respected. Feedback mechanisms offered by Internet user groups, Internet service provider associations, data protection authorities or other bodies are important ways of ensuring that these guidelines are respected. Contact them if you need clarification or remedies.

3. These guidelines apply to all types of information highways.

- sensitive data and traffic data, on condition that the person concerned has given his or her explicit consent;

- other data, where communication is necessary to fulfil the legitimate purpose or where the person concerned, after having been informed, does not oppose it.

[9] For example, do not store billing data unless this is provided for by law.

[10] See footnote 10.

[11] See footnote 11.