

5093/98/EN/final
WP 17

**Working Party on the Protection of Individuals
with regard to the Processing of Personal data**

Recommendation 1/99

**on Invisible and Automatic Processing of Personal Data on the Internet
Performed by Software and Hardware**

Adopted by the Working Party on 23 February 1999

Recommendation 1/99
on Invisible and Automatic Processing of Personal Data on the Internet
Performed by Software and Hardware

Adopted by the Working Party on 23 February 1999

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD
TO THE PROCESSING OF PERSONAL DATA

Set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

Having regard to Articles 29 and 30 paragraph 3 of that Directive,

Having regard to its Rules of Procedure and in particular to Articles 12 and 14 thereof,

HAS ADOPTED THE PRESENT RECOMMENDATION:

1. The Working Party encourages the software and hardware industry to work on Internet privacy-compliant products that provide the necessary tools to comply with the European data protection rules.

A condition for legitimate processing of personal data is the requirement that the data subject is informed and thus made aware of the processing in question. Therefore, the Working Party is especially concerned about all kinds of processing operations which are presently being performed by software and hardware on the Internet without the knowledge of the person concerned and hence are "invisible" to him/her.

Typical examples of such invisible processing are the "chattering" at the HTTP level¹, automatic hyperlinks to third parties, active content (like Java, ActiveX or others client based scripting technologies) and the cookies mechanism as currently implemented in the common browsers.

2. Internet software and hardware products should provide the Internet users information about the data that they intend to collect, store or transmit and the purpose for which they are necessary.

Internet software and hardware products should also give the capacity to the data user to easily access any data collected about him/her at any later stage.

This means for example:

¹ This means that information is sent in the http request which is exceeding the information necessary in order to contact the server.

- In the case of browser software that, on establishing a connection with a web server (sending a request or receiving a Web page) the user is informed of which information is intended to be transferred and for what purposes.
 - In the case of hyperlinks sent by a web site to a user by whatever means, it would mean that the user's browser should reveal them all to the user.
 - In the case of cookies, the user should be informed when a cookie is intended to be received, stored or sent by the Internet Software. The message should specify, in generally understandable language, which information is intended to be stored in the cookie, for what purpose as well as the period of validity of the cookie.
3. The configuration of hard- and software products should not, by default, allow for collecting, storing or sending of client persistent information². For example:
- Browser software should, by default, be configured in such a way that only the minimum amount of information necessary for establishing an Internet connection is processed. Cookies should, by default, not be sent or stored.
 - During its installation, a browser's feature designed to store and send data about user's identity or communication behaviour (profile) should not be filled in automatically with any data previously stored on the user's equipment.
4. Internet hard- and software products should allow the data subject to freely decide about the processing of his/her personal data by offering user-friendly tools to filter (i.e. to reject or to modify) the reception, storage or sending of client persistent information following certain criteria (including profiles, the domain or the identity of the Internet server, the kind and the duration of the information being collected, stored or sent and so on). The user should be provided with clear instructions regarding the use of soft- and hardware for the implementation of these options and tools. For example:
- This means that browser software should provide options so that the user can configure the browser, specifying which information the browser should or should not collect and transmit.
 - This means for cookies that the user should always be given the option to accept or reject the sending or storage of a cookie as a whole. Also the user should be given options to determine which pieces of information should be kept or removed from a cookie, depending on e.g. the period of validity of the cookie or the sending and receiving Web sites.

² Client persistent information is a technical (not legal) term which covers information related to the client (the user's PC) and remaining longer than one session on the computer equipment. A session begins when the client asks for a page on a particular Web site and ends when he decides to turn off the browsing program or the computer or when he asks for a page of another Web site. Cookies are typical client persistent information, the same is true for privacy preferences.

5. Internet software and hardware products should allow the users to remove client persistent information in a simple way and without involving the sender. The user should be given clear instructions on how to do this. If the information cannot be removed, there must be a reliable way to prevent it from being transferred and read.
 - Cookies and other client persistent information should be stored in a standardised way and be easily and selectively erasable at the client's computer.

BACKGROUND

Presently it is almost impossible to use the Internet without being confronted with privacy-invasive features which carry out all kinds of processing operations of personal data in a way that is invisible to the data subject. In other words, the Internet user is not aware of the fact that his/her personal data have been collected and further processed and might be used for purposes that are unknown to him/her. The data subject does not know about the processing and has no freedom to decide on it.

An example of this type of technique is the so-called cookie, which can be defined as a computer record of information that is sent from a web server to an user's computer for the purpose of future identification of that computer on future visits to the same web site.

Browsers are software programs designed to, among other things, graphically display material that is available on the Internet. Browsers communicate between the user's computer (client) and the remote computer where information is stored (Web server). Browsers often send more information to the Web server than strictly necessary for establishing the communication. Classical browsers will automatically send to the Web server visited the type and language of the browser, the name of other software programmes installed on the user's PC and operating system, the referring page, cookies etc. Such data can also be transmitted systematically to third parties by the browser software, in an invisible way.

These techniques allow the creation of clicktrails about the Internet user. Clicktrails consist of information about an individual's behaviour, identity, pathway or choices expressed while visiting a web site. They contain the links that a user has followed and are logged in the web server.

The European data protection directives 95/46/EC and 97/66/EC contain detailed provisions for the protection of individuals with regard to the protection of personal data. Both directives are relevant for the situations dealt within this recommendation because personal data concerning the Internet users are processed in this context. Cookies or browsers can contain or further process data allowing the direct or indirect identification of the individual Internet user.

The application of the provisions on fair processing, legitimate grounds of processing and the right of the data subject to decide on the processing of his/her own data lead to the above recommendation.

The Working Party is especially concerned about the risks inherent to the processing of personal data on data subjects who are completely unaware of such processing. The software and hardware designers are therefore urged to take into account and respect the principles of these directives in order to enhance the privacy of the Internet users.

Done at Brussels, 23 February 1999

For the Working Party

The Chairman

Peter HUSTINX