### ARTICLE 29 - DATA PROTECTION WORKING PARTY



5020/01/EN/Final WP 43

### **RECOMMENDATION 2/2001**

on certain minimum requirements for collecting personal data on-line in the European Union

Adopted on 17 May 2001

The Working Party has been established by Article 29 of Directive 95/46/EC. It is the independent EU Advisory Body on Data Protection and Privacy. Its tasks are laid down in Article 30 of Directive 95/46/EC and in Article 14 of Directive 97/66/EC. The Secretariat is provided by:

## 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<sup>1</sup>,

having regard to Articles 29 and 30 paragraphs 1 (a) and 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:

#### I. Introduction

1. In its working document entitled "Privacy on the Internet – an integrated EU approach to on-line data protection" of 21 November 2001², the Working Party stressed the importance of ensuring that adequate means are put in place to guarantee that individual Internet users get all the information they need to place their trust, in full knowledge of the facts, in the sites with which they enter into contact, and if need be, to exercise certain choices in accordance with their rights under European legislation. This is particularly important given that Internet use multiplies the opportunities for collecting personal data and consequently the risks to the fundamental rights and liberties of individuals, in particular their private life. In its Opinion N° 4/2000 of 16 May 2000 on the level of protection provided by the "safe harbour principles", the Working Party invited the Commission to consider as a matter of urgency the creation of a EU seal system for Internet sites, based on common criteria of data protection assessment that could be determined at the Community level.

This recommendation follows on from the two above-mentioned documents. It aims to contribute to the effective and homogeneous application of the national provisions adopted in compliance with the personal data protection Directives<sup>3</sup>, by providing concrete indications on how the rules set out in the Directives should be applied to the most common processing tasks carried out via the Internet. Such processing occurs, in particular, in the course of "an initial contact" between an Internet user and a website, whether this is solely for the purpose of seeking information or to conclude a commercial transaction on a step-by-step basis.

Official Journal no. L 281 of 23/11/1995, p. 31, available at: http://europa.eu.int/comm/internal\_market/en/media/dataprot/index.htm

WP 37 (5063/00): Working Document - Privacy on the Internet – An integrated EU approach to on-line data protection. Adopted on 21 November 2000.

Available at: <a href="http://europa.eu.int/comm/internal\_market/en/media/dataprot/wpdocs/wp37en.htm">http://europa.eu.int/comm/internal\_market/en/media/dataprot/wpdocs/wp37en.htm</a>

Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and Directive 97/66/EC of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector. Available at: http://europa.eu.int/comm/internal\_market/en/media/dataprot/law.htm

The indications given below mainly concern the collection of personal data on the Web and are intended to identify the concrete measures to be put in place by the players concerned for ensuring that processing is fair and lawful (application of Articles 6, 7, 10 and 11 of Directive 95/46/EC). They focus in particular on when, how and which information must be provided to the individual user but add practical details on other rights and obligations arising from the Directives.

The main objective of this Recommendation is thus to give practical added value for the implementation of the general principles of the directive. The Working Party considers the present Recommendation as a first initiative to spell out on the European level a "minimum" set of obligations in a way that can easily be followed by controllers (the natural or legal person responsible for the processing of personal data in the context of a web-site)<sup>4</sup> operating web sites which may need to be completed by adding further detail or subject matter<sup>5</sup>. This does of course not dispense the controllers from their present obligations to check their processing against the full range of requirements and conditions set up in the applicable national law in order to make it lawful.

This recommendation applies, if the controller is established in one of the Member States of the European Union. In that case the national law of the Member State concerned will apply to the processing of personal data in the context of the activities of that establishment. The recommendation also applies, where the controller is not established on Community territory, but for the purpose of processing personal data, makes use of equipment, automated or otherwise, situated on the territory of one of the Member States of the EU. Such processing is covered by the national law of the Member State where the technical facilities or means are situated<sup>6</sup>.

### 2. To achieve this objective, the recommendation is addressed in particular:

\_

For ease of reference, Article 2 of Directive 95/46/EC defines the controller as "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law".

The concrete recommendations made in this recommendation represent minimum requirements in the sense that they are not the only ones. They should be supplemented in future by additional recommendations on the processing of more sensitive personal data, such as processing in connection with health sites, sites addressed to children or portal services. As regards certain other specific processing, such as the dissemination of personal data on a site or the storage of traffic data by Internet service providers or Internet Content and Service providers, reference is made to the Working Party's recommendations in the document mentioned in footnote 1 and to other relevant positions taken by the Working Party, for example WP 25 (5085/99): Recommendation 3/99 on the preservation of traffic data by Internet Service Providers for law enforcement purposes. Adopted on 7 September 1999. WP 18 (5005/99): Recommendation 2/99 concerning the privacy in the context of interceptions. Adopted on 3 May 1999. WP 17 (5093/98): Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet performed by Software and Hardware. Adopted on 23 February 1999. All available at: see footnote 1.

cf. Article 4 1(a) and (c) of Directive 95/46/EC. This should be clearly distinguished from the question whether personal data may be lawfully transferred from the EU to a third country. That question is dealt with by Articles 25 and 26 of Directive 95/46/EC, and the related decisions of the European Commission concerning the adequacy of the level of protection in a third country. For instance, if an American website makes use of equipment within the EU to collect and process personal data, the legislation of the European country in question will apply to the collection, and processing operations, irrespective of whether this company is or not considered to provide an adequate level of protection, in accordance with the decision of the EU Commission regarding the Safe Harbour. This question whether a data recipient has adhered to the Safe Harbour will only be relevant for the lawfulness of the subsequent transfers of personal data from a company established in the EU to that company.

- to the <u>controllers</u> collecting data on-line, by supplying them with a practical guide listing the minimum set of concrete measures to be put in place;
- to <u>individual Internet</u> <u>users</u> so that they are informed about their rights and can exercise them;
- to the <u>bodies wishing to award a label</u> certifying conformity of the processing procedures used with the European data protection Directives, by providing them with reference criteria for awarding such a label as regards the information to be given and the collection of personal data. It goes without saying that in addition to these reference criteria, other criteria concerning other obligations and rights must necessarily be taken into account also when awarding labels. The Working Party will publish a comprehensive document on this question later;
- to the <u>European data protection authorities</u> in order to provide them with a <u>common</u> reference frame for their task of checking compliance with the national provisions adopted by Member States in accordance with the above mentioned Directives.
- 3. In addition, the Working Party is of the opinion that this recommendation should also serve as reference for <u>developing standards for software and hardware intended</u> for the collection and processing of personal data on the Internet.

# II. Recommendations on the information to be provided when personal data are collected on the territory of European Union Member States.

- 2.1. What information should be provided to the data subject and when?
- 4. Any collection of personal data from an individual via a web site implies prior supply of certain information. In terms of content, compliance with this obligation makes it necessary:
- 5. to state the identity and physical and electronic address of the controller and, where applicable, that of the representative appointed pursuant to Article 4.2 of the Directive;
- 6. to state clearly the purpose(s) of the processing for which the controller is collecting data via a site. For example, when data are collected both to execute a contract (Internet subscription, ordering a product, etc) and also for direct marketing, the controller must clearly state these two purposes;
- 7. to state clearly the obligatory or optional nature of the information to be provided. Obligatory information is information, which is necessary to carry out the service requested. The obligatory or optional nature could be indicated, for example, by a star referring to the obligatory nature of the information, or alternatively, by adding "optional" besides non-obligatory information. The fact that the data subject does not supply optional information cannot count against him/her in any way;
- 8. to mention the existence of and conditions for exercising the rights to consent or to object, as the case may be, to the processing of personal data<sup>7</sup> as well as to access and

4

A processing for a specified purpose is only legitimate if it is based on one of the grounds enumerated in Article 7 of Directive 95/46/EC (*inter alia* if the individual concerned has unambiguously given his consent, if the processing is necessary for the performance of a contract with the individual concerned, if processing is necessary for compliance with a legal obligation of the controller, if necessary for the purposes of the

to rectify and delete data. Information should be provided firstly regarding the person or service to be addressed to exercise these rights and secondly regarding the possibility of exercising them both on-line and at the physical address of the controller;

9. to list the recipients or categories of recipients of the collected information. When collecting any data, the sites should state whether the collected data will be disclosed or made available to third parties - such as business partners, subsidiaries etc. in particular –and why (for purposes other than providing the requested service and for the purposes of direct marketing<sup>8</sup>).

If this is the case, the Internet users must have a real possibility of objecting to this <u>online by clicking a box</u> in support of disclosure of data for purposes other than providing the requested service. Since the right to object can be exercised at any time, the possibility of exercising it on line should also be mentioned in the information provided to the data subject. Conscious of the disadvantage of over-loading the screens with information, the Working Party is of the opinion that where there is no mention of recipients, this is equivalent to the controller undertaking not to communicate or disclose the information collected to third parties whose name and address have not been provided, unless the identity of the third party is obvious and the communication of the data to it is strictly necessary to provide the service requested by the internet user and the disclosure is made only for that purpose.

- 10. Where it is anticipated that the data will be transmitted by the controller to countries outside the European Union, to indicate whether or not that country provides adequate protection of individuals with regard to the processing of their personal data within the meaning of Article 25 of Directive 95/46/EC. In that case, specific information must be provided on the identity and address of the recipients (physical and/or electronic address)<sup>2</sup>;
- 11. to give the name and address (physical and electronic address) of the service or person responsible for answering questions concerning the protection of personal data;
- 12. to mention clearly the existence of automatic data collection procedures, <u>before</u> using such a method to collect any data <sup>10</sup>.

legitimate interests pursued by the controller or by the third party to whom the data are disclosed unless the interest of the individual concerned is prevailing).

The right to object (see Article 14) shall be granted by Member States at least in two situations covered by Article 7 including the last one cited above. The individual has the right, save where otherwise provided by national law, to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him. The right to object on request and free of charge exists in any case when the processing in question is intended for the purposes of direct marketing. In addition the data subject can also object free of charge (once informed and from the first disclosure) to personal data being disclosed to third parties or used on behalf of third parties for the purposes of direct marketing.

- Disclosure to third parties may be authorised only if the anticipated purpose is not incompatible with that for which the data were collected and if it is based on one of the grounds enumerated in Article 7 which make the processing legitimate.
- Information regarding adequacy decisions is available on the Commission website at the following address: <a href="http://europa.eu.int/comm/internal\_market/en/media/dataprot/index.htm">http://europa.eu.int/comm/internal\_market/en/media/dataprot/index.htm</a>.
- "Invisible" and automatic processing of Personal Data is subject to the same terms, conditions and guarantees as other processing of personal data. See Recommendation 1/99 of the Working Party on Invisible

Where such procedures are used, the data subject must be given the information mentioned in this document. In addition, he/she should also be informed of the domain name of the site server transmitting the automatic collection procedures, the purpose of these procedures, their period of validity, whether or not acceptance of such procedures is necessary to visit the site and the option available to any Internet user to object to their use, as well as the consequences of de-activating such procedures. In cases where other data controllers are involved in collection of personal data, the data subject should be provided with information on the data controller's identity, purposes of processing in relation to each data controller.

The information and the possibility of opposing to the collection must be communicated <u>before</u> using any automatic procedures, which trigger the user's PC to connect to another Website. e. g. when the user is automatically led by one website to contact another to view advertising in the form of "banners" to avoid that this second site could collect data without any knowledge of the user.

For example if a cookie is placed by the server of a controller, the information must be provided before it is being sent to the Internet user's hard disk in addition to the information provided by existing technology which is limited to automatically giving the name of the transmitting site and the period of validity of the cookie.<sup>11</sup>

- 13. To point out the <u>security measures</u> guaranteeing the authenticity of the site, the integrity and confidentiality of the information transmitted over the network taken in application of the national legislation applicable. 12
- 14. The information should be provided in <u>all the languages used on the site and in particular at those places where personal data are to be collected.</u>
- 15. The controllers should check the consistency of the information contained in the various "documents" which commit the site ("personal data and privacy protection" heading, electronic forms, text relating to the general conditions of sale and other commercial communications).
  - 2.2. How should the information be provided?
- 16. The Working Party considers that, the following information should be shown directly on the screen before the collection in order to ensure fair processing of data. This information concerns:
  - the identity of the controller;
  - the purpose(s);
  - the obligatory or optional nature of the information requested;

and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware (23 February 1999), available on the website mentioned in footnote 1.

If a cookie is placed by an organisation through its own website and only this organisation can access the content of the cookie, there is no additional requirement for information identifying the organisation responsible for placing the cookie to be given, provided that the organisation hosting the website has already been adequately identified.

See the specific rules in Article 17 (1) and (3), second indent of Directive 95/46/EC.

- the recipients or the categories of recipients of the collected data;
- the existence of the right of access and rectification;
- the existence of the right to oppose any disclosure of the data to third parties for purposes other than the provision of the requested service and the way to do so (for example, by placing a box to be ticked)
- the information which must be supplied when using automatic collection procedures;
- the level of security during all processing stages including transmission, for example over networks.

In such cases, the information should be provided interactively and on screen. Thus, in the case of automatic data collection methods, if necessary this information could be provided using the technique of a "pop-up" window.

As regards the level of security during the transmission of the data from the user's equipment to the web site, this might be a heading such as "You are entering a secure session" or the automatic information procedures present in the navigators, such as the appearance of specific icons in the form of a key or a padlock.

17. Furthermore, the Working Party considers that complete information on the privacy policy (including the way to exercise the right of access) should be directly accessible on the home page of the site and anywhere where personal data are collected on-line. The title of the heading to click on should be sufficiently highlighted, explicit and specific to allow the Internet user to have a clear idea of the content to which he/she is being sent. For example, the heading could state "We are collecting and processing personal data relating to you. For further information, click here" or "Personal Data or Privacy Protection". The content of the information to which the Internet user is directed should also be sufficiently specific.

### 3. Recommendations for implementing other rights and obligations

The Working Party would also like to draw the attention of the addresses of this Recommendation to some other rights of the individuals and obligations of controllers based on the directives which are of particular relevance in the context of collecting personal data on web sites. As with the indications on information, the Working Party considers that the recommendations below are of immediate practical value for both controllers and Internet users.

- 18. Collect only data as far as necessary in view of achieving the purpose specified;
- 19. ensure that data is processed only in so far as it is legitimate on the basis of one of the criteria enumerated in article 7 of the directive 95/46/EC;
- 20. ensure effective exercise of the <u>right to access and to rectify</u>, rights which it should be possible to exercise both at the physical address of the controller and on-line. Security measures should exist to guarantee that only the data subject has on-line access to the information, which concerns him/her;
- 21. implement the "finality" or "purpose" principle, which requires personal data only, be used where necessary for a specific purpose. In other words, without a legitimate reason, personal data cannot be used and the individual remains anonymous (Article

- 6 (1) b of Directive 95/46/EC). This principle is also sometimes called "data minimisation principle".
- 22. In the same context as described under point 21, provide for and promote anonymous consultation of a commercial site without requests for identification of the users by name, first name, e-mail address or other identifying data.

Where a link to a person is needed without however full identification, propose and accept the use of pseudonyms of all kinds.

Where no legal identification requirement exists, promote and accept the use of <u>pseudonyms</u>, <u>even</u> in the case of certain transactions. One example is the use of pseudonym certificates for electronic signatures (see Article 8 of Directive 1999/93/EC on a Community framework for electronic signatures).

- 23. Fix a storage period for the data collected. Data can only be kept for as long as this is justified by the purpose of the processing specified and pursued (Article 6 of Directive 95/46/EC and Article 6 of Directive 97/66/EC).
- 24. Take the steps necessary to ensure data security during processing including transmission (for example restrict and define the persons authorised to have access to the data, use strong encryption etc. Article 17 of Directive 95/46/EC).
- 25. Where a processor is involved, for example to host a web site, conclude a contract requiring the processor to put in place appropriate security measures in accordance also with the law of the Member State where the processor is located and only process personal data on the data controller's instructions.
- 26. As appropriate under national law, notify the supervisory authority (when the site controller is established in the European Union or when he has a representative in the European Union). The registration number of the notification can appear on the site, to great advantage, under the heading dedicated to data protection.
- 27. When transferring information to a third country where adequate protection is not guaranteed, ensure that the transfer of data only takes place if it is in line with one of the derogations provided for in Article 26 of Directive 95/46/EC. In such cases, inform the individual about the adequate guarantees provided in order to make the transfer lawful.

# 4. Collection of addresses for direct marketing by e-mail and the dispatch of newsletters

### 28. As regards direct marketing by e-mail:

- the Working Party reiterates its view that e-mail addresses picked up in public areas of the Internet such as news groups without the informed knowledge of the individual are not lawfully collected. They can thus not be used for any other

purpose than the one for which they have been made public, in particular not for direct marketing. <sup>13</sup>

- use of e-mail addresses for direct marketing solely where these have been collected fairly and lawfully. Fair and lawful collection implies that the data subjects have been informed of the possibility of this information being used for commercial direct marketing and that they have been placed in a position to consent to such use directly at the time the information is collected (click box on line)<sup>14</sup>. The sending of e-mail of a promotional nature under these conditions must also be accompanied by the possibility of on-line withdrawal from the mailing list used<sup>15</sup>.

### 29. As regards the dispatch of newsletters:

- Secure the prior agreement of the data subjects and ensure that they can effectively unsubscribe at any time, which will require informing them of this possibility each time a newsletter is sent.

The Working Party invites the Council, the European Commission, the European Parliament and Member States to take into account this Recommendation.

The Working Party reserves the possibility to issue further comments.

Done at Brussels, 21 May 2001

For the Working Party

The Chairman

Stefano RODOTA

13

See WP 28 (5007/00): "Opinion 1/2000 on certain data protection aspects of electronic commerce", adopted on 3.2.2000, WP 29 (5009/00): "Opinion 2/2000 concerning the general review of the telecommunications legal framework", adopted on 3.2.2000, and, in particular, as to the application of Articles 6 and 7 of Directive 95/46/EC, WP 36 (5042/00): "Opinion 7/2000 on the European Commission proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2000 (COM(2000)385)", adopted on 2.11.2000 and WP 37 (5063/00): "Working document: Privacy on the Internet, an integrated approach to online data protection", adopted on 21.11.2000.

Within the European Union, five Member States (Germany, Austria, Italy, Finland and Denmark) have adopted measures aimed at banning unsolicited commercial communications. In the other Member States, either an opt-out system exists or the situation is not fully clear. It should be noted that the Commission proposal for a directive on the processing of personal data and the protection of privacy in the electronic communications sector (COM(2000)385) of 12 July 2000 favours a harmonised solution based on the "optin" approach which had been unanimously supported by the Working Party in its Opinion 7/2000 (WP 36 cited above); see also the study of S. Gauthronet and E. Drouard (ARETE) for the Commission, "Unsolicited Commercial Communications and Data Protection, January 2001, available at: http://europa.eu.int/comm/internal\_market/en/media/dataprot/studies/spamsum.htm.

Additional requirements concerning unsolicited commercial communications in cases where opt-out is allowed on the basis of Directive 97/66/EC are laid down in the Directive on electronic commerce.