5035/01/EN/Final
WP 56

Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites

Adopted on 30 May 2002

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[1],

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 working document:

1. Introduction

The objective of this document is to discuss the question of the international application of EU data protection law to the processing, in particular the collection, of personal data by web sites, which are based outside the European Union[2]. This working document aims at being a useful tool and point of reference for controllers and those advising them when considering cases involving processing of personal data on the Internet by non-EU based web sites. As this is a very complicate area and Internet a very dynamic environment, this document will not offer definitive solutions concerning all possible issues related to this question.

In its Working document "Privacy on the Internet"[3], the Article 29 Data Protection Working Party identified a clear need to specify the concrete application of the rule on applicable law of the general data protection directive (Article 4 paragraph 1 (c))[4], in particular to on-line processing of personal data by a controller established outside the Community. National data protection supervisory authorities are regularly requested to advise business and individuals on this subject.

The need to determine whether national law applies to situations with links to several countries is not specific to data protection, or to the Internet, or to the European Union. It is a general question of international law, which arises in on-line and off-line situations where one or more elements are present that concern more than one country. A decision is required on what national law is to be applied before a solution on substance can be developed.

---

[1] Official Journal no. L 281 of 23/11/1995, p. 31, available at: http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

[2] The data protection Directive 95/46/EC has also been implemented within the European Economic Area (EEA). The reference to the European Union in this document should be understood as referring also to the EEA.

[3] "Privacy on the Internet - An integrated EU Approach to On-line Data Protection", WP 37, 21 Nov. 2000

[4] Directive 95/46/EC of the European Parliament and of the Council 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 O.J. n° L 281 of 23.11.1995, p. 31-50., available at: http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html

These decisions involve consideration of a number of factors. First and foremost, the concern of a given State is to protect the rights and interests of its citizens, residents, industry and other constituencies recognised under national law. In many countries, penal law (which is the reverse of laws granting rights and freedoms) claims the most extensive application with international effects. Prominent cases such as Yahoo![5] or CompuServe[6] illustrate how Courts apply domestic penal law to prohibit access to pornographic or racist content on foreign Internet servers. A recent decision of the German Supreme Court in penal matters condemned a publisher of the "Auschwitz Lüge" (denial of the existence of Auschwitz) on an Australian web site even though it was not proven that this site was actually accessed from Germany[7]. According to the Court, in the context of this particular crime, it is sufficient that the Internet content is "able" to adversely affect the public order in Germany, it is not necessary that it effectively happened.

Such international effects of protective rules express generally the concern of the legislator or of the judge to protect citizens where necessary in spite of the intrinsic difficulties of enforcement linked to the cross-frontier situation involved and to apply them in practice in order to ensure that the aim pursued is reached.

At the level of EU law, several examples illustrate such a search for coherence.

In the field of competition law, the European Commission can make decisions affecting companies established outside the EU where they do business within the EU. A good example of this was the recent decision of the Commission[8] to block the proposed merger[9] between General Electric and Honeywell, two US companies. This decision, made in July 2001, declared in Article 1 that a merger between the two companies would create a 'concentration incompatible with the Common Market'. The Commission established that the two companies had a combined community wide turnover of more than EUR 250 million and therefore concluded that the notified operation has a 'community dimension'.

The extra-territorial dimension of Community law can also be seen in the area of consumer law. Article 12 of the distance selling Directive[10] states that a consumer will not lose the protection that he is granted by the Directive by virtue of a choice of law clause in a contract where the law of the chosen non member country provides less protection than that of EU law. This is the case where the contract has a 'close connection' with one or more Member States[11]. The phrase 'close connection' is taken

---

[5] TGI Paris, *ordonnance du référé* of 20 November 2000 http://legal.edhec.com/DTIC/Decisions/Dec_responsabilite_0.htm

[6] AG München, judgement of 28.05.1998 – 8340 Ds 465 Js 173158/95

[7] BGH, judgement of 12.12.2000, Az: 1 StR 184/00.

[8] Decision of 3/7/01 Case No. COMP/M2220 made pursuant to Article 8(3) of Regulation (EEC) No. 4064/89 Merger Procedure

[9] Under the notified agreement Honeywell was to become a wholly owned subsidiary of General Electric

[10] Directive 97/7/EC

[11] Article 6(2) of Directive 93/13 on unfair terms in consumer contracts and Article 7(2) of Directive 99/44 on certain aspects of the sale of consumer goods and associated guarantee are very similar to Article 12(2). They both insist on the application of EU law and they both use the term 'close connection'.

from Article 7 of the Rome Convention of 1980. This Article states that 'mandatory rules' of a country must be applied to situations, which are governed by the law of a different state where that situation has a 'close connection' with the country.

Furthermore, there has been case law, which follows a similar reasoning regarding the Commercial Agents Directive[12]. The European Court of Justice has ruled[13] that where a commercial agent that carries on his activity within the Community is employed by a principal established outside the Community, that principal cannot avoid the requirements of the Directive by means of a contractual clause stipulating that a third country's law applies to the relationship. The court stated that Community law must apply in cases where 'the situation is closely connected with the Community'.

A further, more practical example can be found in the airline industry. The Council has produced a Regulation entitled the Code of Conduct for CRS's (Computer Reservation Systems)[14]. This Regulation (which governs the way, in which CRS systems are used) applies to 'any computerised reservation system…. when offered for use or used in the territory of the Community, irrespective of the status or nationality of the system vendor or the location of the relevant central data processing unit'. Hence when a system can be accessed from the EU, even if the central equipment of the system is not located in the EU (and data are fed into this system via terminals in the EU or otherwise), EU law automatically applies.

Hence from an examination of the applicability of EU law to these cases with an extra territorial dimension it can be concluded that similar criteria are generally applied. Whether it is a requirement that the relationship have a 'community dimension' or 'close connection' with the Community, in certain situations the European Court of Justice, the European Parliament and Council as well as the European Commission see fit to impose EU rules on non EU based entities.

In other countries, for example in the United States of America, courts and laws apply similar reasoning in order to subject foreign web sites to local rules : The US Children's Online Privacy Protection Act 1998 (COPPA) also applies to foreign web sites collecting personal information from children on US territory[15]. Under this Federal law, the operator of a web site, which is directed towards children under the age of 13 (or of a site, which has a general audience, but where the operator has actual knowledge that the site is collecting information from children) is obliged to comply with the provisions of the COPPA. This Act governs what information an operator must give in a privacy policy, when and how an operator is obliged to seek verifiable consent from a parent and what responsibilities an operator has to protect children's privacy and safety online. What is interesting for the present purpose is that this law applies not specifically to US companies, but to companies 'located on the Internet' and therefore in terms of the Act's jurisdiction it does not matter where the web site is physically located as long as it does business within the US. If this is the case, the web site will be subject to US law in this area.

[12] Directive 86/653/EEC

[13] Ingmar GB Ltd. and Eaton Leonard Technologies Case C-381/98

[14] Code of Conduct for CRS's (combined version of Council Regulations no. 2299/89 as amended by 3089/93 as amended by 323/99)

[15] 15 U.S.C. § 6502 (1)(A)(I), referred to in Joel R. Reidenberg, see footnote 5.

A survey of international law suggests that States have a tendency to use several alternative criteria for determining extensively the scope of application of national law, in order to cover as many cases as possible in the interest of protecting as broadly as possible national consumers and industry. Inevitably, this tendency results in the application of several national laws to a situation involving a cross-frontier element. International legal instruments therefore try to determine the relevant criteria in a neutral and non-discriminatory way. However, the most recent attempt to progress on a draft convention on the applicable law to contracts under the auspices of the "The Hague Conference" failed, because countries could not agree on the decisive criterion. This indicates the heart of the problem when discussing the applicable law: a fair balance has to be struck between the various interests of the countries involved.

Against this background, it has to be noted that the EU data protection directive contains an explicit provision on the applicable law indicating a criterion. Irrespective of whether this provision is easy to understand or to handle, it is nevertheless an advantage for the benefit of individuals and business that the data protection directive addresses this essential question.

2. Article 4 of Directive 95/46/EC on applicable law

Article 4 of the Directive reads as follows: National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions, which could be initiated against the controller himself.

This Article discusses the cases giving rise to the question of the applicable law to personal data processing operations: these are cases where at least one aspect of processing of personal data goes beyond one Member State alone. For example: a direct marketing company compiles mailing lists on consumers in several Member States and uses them in one Member State to enable the sending of advertising to these consumers. Or, a US web site puts a cookie on the personal computer of individuals in the EU in order to identify the PC to the web site in view of linking up that information with others.

The directive distinguishes in general terms between, on the one hand, situations where the cross-frontier elements are confined to EU Member States or with territories outside the geographical borders of the European Union, but where the law of a Member State applies by virtue of international public law (the "diplomatic case")[16] and, on the other hand, situations where the processing involves elements going beyond the borders of the European Union[17].

Concerning the situations within the Community, the objective of the directive is twofold: it aims at avoiding gaps (no data protection law would apply) and at avoiding multiple/double application of national laws. As the directive addresses the issue of applicable law and establishes a criterion for determining the law on substance that should provide the solution to a case, the directive itself fulfils the role of a so-called "rule of conflict" and no recourse to other existing criteria of international private law is necessary.

In order to find an answer, the directive uses the criterion or « connection factor » of the "*place of establishment of the controller*" or, in other words, the country of origin principle typically applied in the Internal Market. This means concretely:

When the processing is carried out in the context of the activities of an establishment of the controller on the territory of one Member State, the data protection law of this Member State applies to the processing.

When the same controller is established on the territory of several Member States, each of the establishments must comply with the obligations laid down by the respective law of each of the Member States for the processing carried out by them in course of their activities. It is not an exception to the country of origin principle. It is merely its strict application: where the controller chooses not to have only one, but several establishments, he does not benefit from the advantage that complying with one law is enough for his activities throughout the whole Internal Market. This controller then faces the parallel application of the respective national laws to the respective establishments. The Working Party might deal with this issue in the future.

The application of the country of origin principle is justified in an Internal Market where national data protection laws afford equivalent protection thanks to the harmonisation of the data protection rights of individuals and obligations of industry and other controllers of processing of personal data. In such a way the country of origin principle, which is in some way a restriction of the scope of application of the data protection laws of the Member States, does not have adverse effects on the rights and interests of its residents or industry. In effect, even if the Member States laws are not applicable to all processing involving a national data subject or taking place on the national territory, the fact that the law of another Member State alone is applicable, has a very limited impact, given that both laws are harmonised by the directive and thus equivalent. Additionally, co-operation

[16] This case will not be dealt with in this document. It should also be noted that the directive and thus Article 4 apply both to private and public sector processing of personal data falling under Community law. This working document however does not deal with the application of Article 4 to public sector cases.

[17] This distinction applies mainly to the controller. It should in any case be clarified that the applicability of the directive is not affected by the fact that a controller in the EU has a processor operating outside the EU. In that case the directive still applies to the whole of the processing operations.

between national data protection authorities ensures trust, confidence and effective enforcement, whatever the law applicable. [18]

The situation is different as regards processing operations, which involve a controller in a third country. The national laws of these third countries are not harmonised, the directive is not applicable in these countries and the protection of individuals with regard to the processing of their personal data may therefore be missing or weak. The country of origin principle, which is linked to the establishment of the controller, can no longer serve the purpose of determining the applicable law. It is necessary to switch to another connection factor. The European Parliament and the Council decided to come back to one of the classic connection factors in international law, which is the physical link between the action and a legal system. The EU legislator chose the country of the territorial location of equipment used[19]. The directive therefore applies when the controller is not established on Community territory, but decides to process personal data for specific purposes and makes use of equipment, automated or otherwise, situated on the territory of a Member State.

The objective of this provision in Article 4 paragraph 1 lit. c) of Directive 95/46/EC is that an individual should not be without protection as regards processing taking place within his country, solely because the controller is not established on Community territory. This could be simply, because the controller has, in principle, nothing to do with the Community. But it is also imaginable that controllers locate their establishment outside the EU in order to bypass the application of EU law.

It is worth noting that it is not necessary for the individual to be an EU citizen or to be physically present or resident in the EU. The directive makes no distinction on the basis of nationality or location because it harmonises Member States laws on fundamental rights granted to all human beings irrespective of their nationality. Thus, in the cases that will be discussed below, the individual could be a US national or a Chinese national. In terms of application of EU data protection law, this individual will be protected just as any EU citizen. It is the location of the processing equipment used that counts.

The Community legislator's decision to submit processing that uses equipment located in the EU to its data protection law thus reflects a true concern to protect individuals on its own territory. At international level it is recognised that states can afford such protection. Article XIV of the GATS allows to lay down exemptions from the free trade rules in order to protect individuals with regard to their right to privacy and data protection and to enforce this law.

The next sections explains the terms that are relevant in order to determine the applicable law:

[18] See Article 28 paragraph 6 first sentence of Directive 95/46/EC: "Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3.", and last sentence of the same paragraph on their obligation to co-operate.

[19] This is not the case if the equipment is only used for the purpose of transit through the territory of the Community.

2.1 Establishment

The notion of establishment is relevant in Article 4 (1) c of the directive in the sense that the controller is not established on Community territory. The place, at which a controller is established, implies the effective and real exercise of activity through stable arrangements and has to be determined in conformity with the case law of the Court of Justice of the European Communities. According to the Court, the concept of establishment involves the actual pursuit of an activity through a fixed establishment for an indefinite period[20]. This requirement is also fulfilled where a company is constituted for a given period.

The place of establishment of a company providing services via an Internet web site is not the place, at which the technology supporting its web site is located or the place at which its web site is accessible, but the place where it pursues its activity[21]. Examples are: a direct marketing company is registered in London and develops its European wide campaigns there. The fact that it uses web servers in Berlin and Paris does not change the fact that it is established in London.

2.2. The controller

The *controller* is a general notion from the directive, determining the natural or legal person that alone or jointly with others determines the purposes and means of the processing of personal data (Article 2 (d) of Directive 95/46/EC). The definition is neutral as regards the point of establishment of the controller. It is comprehensive because all processing must be attributable to one or several controllers. In the context of Article 4 (1) c of the directive, this means that there has to be a controller somewhere in the sense of the directive. It seems also necessary that the processing takes place in the course of an activity, which falls within the scope of Community law and thus under the directive. Processing by a natural person in the course of a purely personal or household activity does not fall under the scope of the directive.

To trigger Article 4 (1) c of the directive, the controller has to "*make use of* equipment for the purposes of processing personal data" (and not only for transit), which is situated on the territory of a Member State[22]. This seems to suggest that the controller is active and possesses a particular intent. His decision about the purposes and the means of processing thus comprises this aspect.

[20] Case C-221/89 Factortame [1991] ECR I-3905 §20.

[21] Directive 2000/31/EC, Recital 19.

[22] It has to be noted that there is a difference between the word used in the English version of Article 4 (1) c 'equipment', and the word used in other versions of Article 4 (1) c, which are more akin to the English word, 'means'. The terminology used in other versions of Article 4 (1) c is consistent with the wording of Article 2 (d) defining the controller: the person who decides about the purposes and the "means" of the processing. It should however be recognised that the English text of the directive in previous versions (for instance, in the amended proposal of 1992) also used the term "means" and that this was modified in the course of the negotiations, at quite a late stage, into the term "equipment", as it can be seen in the text of the common position of March 1995.

2.3. Equipment

The Directive does not contain a definition of this term. According to the Collins English dictionary, "equipment" is defined as a set of tools or devices assembled for a specific purpose.
Examples of equipment are personal computers, terminals and servers, which may be used for nearly all kind of processing operations.

The Directive makes clear that *equipment* as such can be automated or otherwise as far as it is not used only for transit of information through the territory of the Community.

A typical case where equipment is used for transit only are the telecommunications networks (back bones, cables etc.), which form part of the Internet and over which Internet communications are travelling from the expedition point to the destination point.

2.4. Making use of equipment

The determination of when “the controller makes use of equipment for the purpose of processing personal data” in Article 4 (1) (c) of the directive is a decisive element for the application of the data protection law in the EU.

The Working Party would advocate a cautious approach to be taken in applying this rule of the data protection directive to concrete cases. Its objective is to ensure that individuals enjoy the protection of national data protection laws and the supervision of data processing by national data protection authorities in those cases where it is necessary, where it makes sense and where there is a reasonable degree of enforceability having regard to the cross-frontier situation involved.

With this in mind, the Working Party is of the opinion that not any interaction between an Internet user in the EU and a web site based outside the EU leads necessarily to the application of EU data protection law. The Working Party has put forward the view that the equipment should be at the disposal of the controller for the processing of personal data.

At the same time, it is not necessary that the controller exercise full control over the equipment. The extent, to which it is at the disposal of the controller, can vary. The necessary degree of disposal is given if the controller, by determining the way how the equipment works, is making the relevant decisions concerning the substance of the data and the procedure of their processing. In other words, the controller determines, which data are collected, stored, transferred, altered etc., in which way and for which purpose.

The Working Party considers that the concept of “making use” presupposes two elements: some kind of activity undertaken by the controller and the intention of the controller to process personal data. This implies that not any “use” of “equipment” within the European Union leads to the application of the Directive.

The power of disposal of the controller should, however, not be confused with property or ownership of the equipment, either of the controller or of the individual. In fact, the directive does not attach any relevance to the ownership of any equipment.

The interpretation presented by the Working Party is fully in line with the motivation for the provision in Article 4 (1) c of the directive given by the EU legislator. Recital 20

explains that "*the fact that the processing is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this directive; whereas in these cases, the processing should be governed by the law of the Member State, in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice"*. This is the corollary, which is necessary in order to reach the Directive's broader objective, which is *"to ensure that individuals are not deprived of the protection to which they are entitled under this Directive"*.

3. Practical examples

This chapter aims at translating the guidance provided for in Article 4 into concrete solutions in typical cases. One element that is common to the cases discussed below is that the Internet user does not necessarily always know whether the web site he will visit and provide data to (either unknowingly or consciously) is situated in the EU or elsewhere. The domain names without geographical elements cannot be physically located without additional information and even for those with geographical elements there is no guarantee that the web site is effectively hosted on a server in the country indicated.

Case A: Cookies

The controller decides to collect personal data by means of a text file (cookie), which is placed on the hard disk of the user's personal computer, while a copy might be kept by the web site or a third party[23]. In the case of further communication, the information stored in the cookie (and therefore in the user PC) is accessed by the web site in order to identify this PC to the controller. The controller is thus enabled to link up all information he has collected during previous sessions with information he collects during subsequent sessions. In this way, it is possible to create quite detailed user profiles.

Cookies are a standard part of HTTP traffic, and can as such be transported unobstructed with the IP-traffic. They contain information about the individual that can be read back by the web site that placed it. A cookie can contain any information the web site wants to include in it: pages viewed, advertisements clicked, user identification number and so on[24].

[23] *Cookies* are pieces of data created by a webserver that can be stored in text files that may be put on the Internet user's hard disk, while a copy may be kept by the website. They are a standard part of HTTP traffic, and can as such be transported unobstructed with the IP-traffic. A *cookie* can contain a unique number (GUI, Global Unique Identifier) which allows better personalisation than dynamic IP-adresses. It provides a way for the website to keep track of a user's patterns and preferences.

The *cookies* contain a range of URLs (addresses), for which they are valid. When the browser encounters those URLs again, it sends those specific *cookies* to the Web server.
Cookies can differ in nature: they can be persistent, but can also have a limited duration, the so-called session *cookies*.

[24] See the book by HAGEL III, J. and SINGER, M., *Net Worth: the emerging role of the informediary in the race for customer information,* Harvard Business School Press, 1999, p. 275.

The SET-COOKIE is placed in the HTTP response header[25], namely in invisible hyperlinks. If a duration is stipulated[26], the cookie will be stored on the Internet user's hard disk and sent back to the web site originating the cookie (or to other web sites from the same sub domain) for that duration. This sending back will take the form of a COOKIE field involved in the browser chattering described above and will take place without any intervention of the user.

As explained above, the user's PC can be viewed as equipment in the sense of Article 4 (1) c of Directive 95/46/EC. It is located on the territory of a Member State. The controller decided to use this equipment for the purpose of processing personal data and, as it has been explained in the previous paragraphs, several technical operations take place without the control of the data subject. The controller disposes over the user's equipment and this equipment is not used only for purposes of transit through Community territory.

The Working Party is therefore of the opinion that the national law of the Member State where this user's personal computer is located applies to the question under what conditions his personal data may be collected by placing cookies on his hard disk.

As was outlined in a previous recommendation of the Working Party[27], the user should be informed when a cookie is intended to be received, stored or sent by Internet Software. The message given to the user should specify, in clear terms, which information is intended to be stored in the cookie and for what purpose as well as the period of validity of the cookie. The user should then be given the option to accept or reject the sending or storage of a cookie as a whole and they should be given options to determine which pieces of information should be kept or removed from a cookie depending on, for example, the period of validity of the cookie, or the sending and receiving web sites[28].

Case B: JavaScript, banners and other similar applications

JavaScripts are software applications sent by a web site to the computer of a user and allow remote servers to run applications on a user PC. Depending on the content of the software, JavaScripts can be used in order to display information on a web page, but also to introduce viruses in the computer (the so-called malicious Java) and/or to collect and process personal data stored in the computer. Where the controller decides to use these

[25] Technically speaking, it is also possible to implement cookies in JavaScript or in the <META-HTTP EQUIV> fields located in the HTML code.

[26] Cookies with no fixed duration are called "session cookies" and disappear when the browser is unloaded or when the socket closes.

[27] Recommendation 1/99 WP 17 'Invisible and Automatic Processing of Personal Data on the Internet performed by Software and Hardware'.

[28] Further information on the nature of cookies and how best to deal with them is provided in the 'Privacy on the Internet - An integrated EU approach to on-line Data Protection' Working Document, WP 37 5063/00. Page 16 contains a general description'Cookies are pieces of data that can be stored in text files that may be put on the Internet user's hard disc, while a copy may be kept by the Website'.
Page 79 details 'Cookie Killers' dealing with both the response by industry to deal with the privacy problems of cookies-the cookie opposition mechanism, and that of privacy activists- independent programmes such as *cookie washer, cookie cutter* and *cookie master*.

tools in order to collect and process personal data, he makes use of equipment in the sense of the Directive, and will have to comply with the provisions of EU legislation.

An advertising company, through an agreement with site owners (e.g. search engine sites) orders the browser (broadly, the computer) of the data subject to connect not only to the search engine he/she wants to visit, but also to the server of the advertising company. This way, the advertising company may be enabled not only to send banners[29] on the screen of the data subject but also, using the browser of the user, to collect address and content data the individual sends to the search engine. The banner ads are placed on the requested web site via an invisible hyperlink to the advertising company[30]. The controller has therefore from the place where he is control over the functioning of the browser, in order to have it connecting and transmitting information to a third party.

In addition to that, to provide the customer with the most „adequate" banner ad, the network advertisers create profiles by using cookies set via the invisible hyperlink. Depending on the configuration of the browser, the user may be aware that the cookie is being placed and may or not give consent. The customer's profile is linked to the identification number of the ad company's cookie so that it can be enlarged every time the customer visits a web site, which has a contract with the advertiser. In that way, additional collection of personal data from the user will take place through his computer and without his intervention every time the Internet user visits the web site that contains the banner.

The directive would also apply to information collected through spywares, which are pieces of software secretly installed in the individual's computer, for instance at the occasion of the downloading of bigger software (e.g. a music player software), in order to send back personal information related to the data subject (e.g. the music titles the individual tends to listen to). These kinds of software programs are popularly known as E.T. applications *"because once they have lodged in the user's computer and learned what they want to know, they do what Steven Spielberg's extra-terrestrial did: phone home"*[31].
This new monitoring software applications often make use of JavaScript and other similar techniques and clearly make use of the equipment of the data subject (computer, browser, hard disc and so on) to collect data and send it back to another location. As these technologies are by definition used without informing the user (the name spyware is clear in that respect) they are a form of invisible and not legitimate processing.

****

The Article 29 Working Party is aware of the fact that, in addition to the two examples mentioned in the previous sections, there are other practical Internet-related cases that might raise difficulties of interpretation, partly due to the technical complexity of some of the systems used.

[29] Banners are small graphic boxes, which appear above or are integrated into the website content.

[30] See for more information chapter 8, Cybermarketing, of WP 37, Privacy on the Internet.

[31] See the cover-page story of Time magazine by COHEN, Adam on 31 July 2000: *How to protect your privacy: who's watching you? They're called E.T. programs. They spy on you and report back by "phoning home". Millions of people are unwittingly downloading them.*

The Working Party will continue to reflect on this matter and might address other practical cases in the light of the national experience and of the technical developments that might play an important role in the future.

It would like to underline that, even in the cases, in which the application of the Directive is not completely clear, the Working Party is committed to continue the dialogue with companies and organisations from third countries who collect personal data in the European Union in order to promote adequate data protection standards for the data subjects.

4. What does this mean in practice?

a) Application of the principles governing the collection of personal data

In all these cases, the application of EU data protection law means among other things the following:

- With a view to making the collection of personal data fair and lawful, the controller has to clearly define the purpose of the processing.

- The controller has also to ensure that the data are adequate, relevant and not excessive in relation to the purpose for which they are collected.

- The collection must be based on a legitimate ground (unambiguous consent, performance of a contract, compliance with a legal obligation, in pursuance of legitimate interests of the controller etc.) and the individual has the right of access to and the rectification or erasure of his personal data.

- The individual has at least to be informed about the identity of the controller and his representative if any, the purpose of the collection, the recipients and about his rights [32].

- Another important aspect is the security of the processing which may require the controller, right from the collection on, to apply specific technical and organisational measures in order to protect the data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the data are transmitted over a network. Such measures shall ensure a level of security appropriate to the risks presented and the nature of the data.

- As regards sensitive data, specific provisions, dealing in particular with security requirements, regulate their collection[33].

[32] Article 10 of the directive states that, where necessary to guarantee fair processing in respect of the data subject, additional information should be given.
In the case of cookies, the individual should have the possibility to accept or refuse the placing of a cookie and he should also have the possibility to determine what data he wishes to be processed by the cookie, what data not.

[33] Some Member States may require prior checking before processing of sensitive data can start.

More details on how the data protection directives apply to data processing by web sites are explained in the Working Party's Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union[34].

b) Procedural aspects

According to Article 4 (2) of Directive 95/46/EC, the controller should furthermore designate a representative who is established on the territory of the Member State where the equipment is located.

Information about the identity of the controller and about the identity of the representative could be easily included in the privacy policy of the web site, or in the general identification information of the responsible of the web site so that the controller responsible for the web site can be easily identified and contacted.

It could be recommended to use widely the possibility that one representative could act on behalf of several controllers or to envisage other pragmatic solutions.

As regards notification of the intended processing operation (namely the collection) to national data protection authorities, the directive provides for choices. According to Article 18 (1) first sentence, the controller or his representative must notify the supervisory authority before carrying out any processing operation or set of operations. Article 19 (1) (a) stipulates that the notification shall include amongst other elements the name and address of the controller and his representative.

According to Article 18 (2) second indent, Member States may provide for a simplification of or exemption from notification in two cases: for categories of processing operations, which are unlikely to affect adversely the rights and freedoms of the data subjects or where the controller appoints a personal data protection official who should ensure, in an independent manner, the internal application of the data protection legislation[35].
The Working Party is aware of the fact that the application of these provisions might pose practical problems and might dedicate further attention to these issues at a later stage.

c) Enforcement

It is obvious that enforcing rules in an international context is not as easy as solely within one given country. The citizen has to be (made) aware of this. Nevertheless, several possibilities exist and can be developed with a view to achieving a reasonable degree of enforcement.

[34] See on substance WP 43 Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union. It should be discussed whether all elements mentioned in WP 43 shall also apply to the on-line collection of data in the EU by controllers established outside the EU.

[35] For the specific provisions of national law implementing this Article of the directive see: http://europa.eu.int/comm/internal_market/en/dataprot/law/impl.htm

A good level of compliance would require in the first instance to make aware both European and international organisations of the requirements of the directive as regards collection of data in the European Union. The widest distribution of this recommendation can only be the first step. It would involve as well technological solutions, providing a pre-established structure for the collection of personal data, which would incorporate the requirements described into the software tools used for the collection of personal data. The Working party has already made reference to the possibility to devise product authorisation procedures, which would include a check of the respect of legal requirements for the protection of personal data. A European system of labels/web seals, open also to non-EU web sites, could be the cornerstone of such action.

Furthermore, in a concrete case, an individual in the European Union who experiences problems with a non-EU web site could submit his case to the competent national data protection supervisory authority. This authority would determine whether the directive, respectively the national data protection law, applies. If it does, the authority could develop contacts with the foreign web site with a view to resolving the problem. If the case is brought before a court in the Member State where the individual is resident, the court will decide whether it can assume jurisdiction over the case (which accordingly to international procedural law could be so, because the party most concerned is the individual living on the same territory as the court). When the court has jurisdiction, it applies Article 4 of Directive 95/46/EC, respectively the relevant national law, transposing it and may find that the foreign web site was processing unlawfully and unfairly the personal data of the individual. Many third countries will already allow to recognise and enforce the judgement, but even if they do not, there exist examples that the foreign web site may nevertheless follow the judgement and adapt its data processing with a view to developing good business practice and to maintaining a good commercial image.

In third countries where data protection rules and authorities are in place enforcement is obviously less problematic.

5. Conclusions

- The Article 29 Data Protection Working Party is of the opinion that an interpretation of the national laws, as expressed in this working document, would be most beneficial with a view to achieving legal security for web sites based outside the European Union. The Working Party is convinced that a high level of protection of individuals can only be ensured if web sites established outside the European Union but using equipment in the EU as explained in this working document respect the guarantees for personal data processing, in particular the collection, and the rights of individuals recognised at European level and applicable anyway to all web sites established in the European Union.

- The Article 29 Data Protection Working Party considers that the development of a programme for the promotion of European data protection rules in a pragmatic way would also help controllers in third countries to better understand, implement and demonstrate privacy compliance. A European system of labels/web seals, open also to non-EU web sites, could be the cornerstone of such action.

- The Article 29 Data Protection Working Party invites the Commission to take into account this working document in its further work.

Done at Brussels, 30 May 2002

For the Working Party

The Chairman

Stefano RODOTA