5075/99/EN/final
WP 23

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

Working document

on the current state of play of the ongoing discussions between the European Commission and the United States Government

concerning

the "International Safe Harbor Principles"

Adopted on 7 July 1999

The following is not an opinion of the Working Party established by Article 29 of Directive 95/46/EC on the Safe Harbor arrangement but simply a message addressed to the Committee created by Article 31 of the Directive which will be meeting on 14th July, expressing some of the Working Party's concerns resulting from its 7th July meeting.

Recalling its previous remarks in opinions 1/99, 2/99 and 4/99 (annexed for ease of reference as annex 1, 2 and 3 respectively):

1. The Working Party, is indeed aware of the importance of the EU-US debate on data protection and of the repercussions that the position finally adopted will have on the majority of other third countries. It is also aware of the time constraints inherent to these discussions and of the difficulties resulting from the differences in the political, economic and cultural approaches.

2. The Working Party has so far diligently examined the successive versions of the Safe Harbor Principles and of the Frequently Asked Questions (FAQs), which have emerged later and which have not yet all been issued, including some of the most important ones. Since having been informed by the Commission that the FAQs are to be an integral part of the Safe Harbor arrangement and to have the same binding force as the Principles, the Working Party considers that henceforth its approach has to be comprehensive with regard to both texts and it should therefore issue an opinion covering both the Principles and the FAQs. It follows that until the Working Party has all the FAQs announced by the American side as well as the related legal texts it will not be able to deliver a complete and definitive opinion on the "Safe Harbor arrangement".

3. Following the discussions on 7th July, the Working Party wishes to draw the attention of the Committee to the following points:

   Legal basis: in the mutual interest of both parties it is advisable to ensure that Article 25 of the Directive is a solid legal basis.

   The scope of the Safe Harbor arrangement : The following should be specified:

   (a) If certain sectors are excluded from the scope of the Safe Harbor mechanism on account of specific provisions (e.g. public sector) or due to the absence of a public monitoring body with responsibility to deal with the subject matter, as required by Article 1 b of the Draft Commission decision (e.g.: employee data, or non-profit-making related activities) and;

   (b) If the organisation in the notification of its adherence to the Safe Harbor, will be able to exclude certain sectors of its own activity (e.g.: online services) and how this will be made public and available to the national supervisory authorities;

   (c) Moreover, the Working Party notes that at present, the level of protection given to the employee data is not satisfactory. Two solutions seem possible: To reinforce overall the level of protection awarded by the Principles or to

exclude this data from the scope of the Arrangement to give it reinforced protection, in view also of the absence of an independent public body as required by Article 1(b) of the draft decision able to deal with this type of data, and ;

(d) Reiterates its concern that the US authorities may derogate from Principles through regulation without giving proper weight to the interests of privacy protection.

The conditions of implementation and enforcement:

(a) What will be the impact on the role of the national supervisory authorities of the choice of an American company to have complaints dealt with by a specific body?

(b) At the European level, when dealing with complaints, what will the respective powers of the national supervisory authorities and of the European Union be?

(c) In the event of simultaneous or successive American and European procedures leading to contradictory positions on a complaint, how will these differences be solved?

(d) The Working Party also notes that the role that the American authorities would wish to be played by national supervisory authorities with regard to those companies that choose to co-operate with them, may pose constitutional, financial, or personnel problems for some national authorities.

(e) Moreover the Working Party considers it advisable to ensure that the verification procedure mentioned in Principle 7 (b) should be independent, that is carried out by a third party, failing which, it considers it advisable to ensure that a report on the verification should be made available to the national supervisory authorities, if necessary.

On the contents of the Principles

While acknowledging certain improvements to the 19 April 1999 text, the Working Party notes that the Principles in their 1st June version do not yet fulfil the requirements of adequate protection. In addition to the questions mentioned in its previous opinions, and in anticipation of its new and comprehensive opinion, the Working Party considers it essential to draw in particular the Committee's attention to the following questions:

Principles 1 and 2 « Notice» and « Choice »

(a) The scope of the purpose principle is different in the Notice Principle and in the Choice Principle.

(b) Comparing with the 4th November 1998 version, the combination of both Principles results now in the possibility for the American companies to use data for another purpose for which it was collected without having to offer choice. Although the directive allows for data to be further processed, provided that the use is not incompatible with the purpose of collection, considering that the « Safe Harbor » Principles do not contain legitimacy of processing criteria, the Wokring Party considers that it is advisable to strengthen the Choice Principle .

Principle 6 « Access »

(a) The exemptions contained in the FAQS are too broad.

(b) Public data needs to be covered.

(c) Data processed in violation of the Principles should be corrected or deleted.

Done at Brussels, 7 July 1999

For the Working Party

The Vice Chairman

Prof. Stefano RODOTA

ANNEX 1: OPINION 1/99

5092/98/EN/final
WP 15

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

OPINION 1/99

concerning
the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government

Adopted by the Working Party on 26 January 1999

Opinion concerning
the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government

The Working Party is aware of the ongoing discussions between the European Commission and the United States Government which are seeking to guarantee both high levels of protection for personal data and the free movement of personal information across the Atlantic. The Working Party attaches importance to these discussions and hopes that it will prove possible to reach a positive outcome as soon as possible. In the light of this discussion, a letter and its annex signed by M. Aaron on 4 November 1998 has been transmitted which contains a certain number of proposals intended to be discussed inside the USA by representatives of US companies with the Federal Department of Commerce. In this context the Working Party urges the parties to these discussions and the EU Member State governments meeting in the committee established by Article 31 of Directive 95/46/EC[1] to take into account the following points.

Data protection rules are not only intended to protect users of new technologies (in particular informatics and Internet) with a view to guaranteeing trust and confidence and thus to provide for the development of these technologies and the exchange of data at international level. These rules express also the adherence to a certain number of fundamental principles and rights based on a common culture of respect for privacy and other values that are inherent in the human being and which is shared equally by the Member States of the European Union and the United States.

1. Privacy and data protection in the United States is found in a complex fabric of sectoral regulation, at both federal and state level, combined with industry self-regulation. Considerable efforts have been made during recent months to improve the credibility and enforceability of industry self-regulation, particularly in the context of the Internet and electronic commerce. Nevertheless, the Working Party takes the view that the current patchwork of narrowly-focussed sectoral laws and voluntary self-regulation cannot at present be relied upon to provide adequate protection in all cases for personal data transferred from the European Union.

2. Given the complexity of the US system of privacy and data protection, the establishment in the US of an agreed "benchmark" standard of protection in the form of a set of "safe harbor" principles offered to all economic actors and US operators is a useful approach which might need to be complemented by contractual solutions in certain specific cases. However, further improvements are needed if free movement of data to the United States is to be ensured on the basis of these privacy principles. In addition, it might be necessary to provide for a methodology which makes clear which companies are covered by the “safe harbor” principles.

[1] 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, JO L 281, 23 November 1995, p. 31. Available at http://www.europa.eu.int/comm/dg15/en/media/dataprot/index.htm.

3. It has to be noted that the decision to adhere to the set of principles belongs solely to the individual company, and so the problem of those companies which do not wish to apply the principles remains whilst no overall legislation exists.

4. Generally, the status of these principles needs to be clarified. Whilst adherence to the principles in the first instance can be voluntary, once a company does decide to adhere and thereby to claim the benefit of "safe harbor", compliance must be compulsory.

5. The credibility of the system is seriously weakened by the lack of a requirement for independent compliance monitoring and by relying solely on company self-certification. Independent verification would need to be serious but could at the same time be practicable, even for small companies. Models currently being developed in the US by the Better Business Bureau OnLine and Trust-E are going in the right direction.

6. It must be possible for complaints from individuals whose data have been transferred from the EU to be dealt with in a practical and effective manner, and adjudicated upon, in the final instance, by an independent body. A key issue in this regard is the identification of one or more independent public bodies or third party organisations in the US that are willing and able to act as contact points for EU data protection authorities and to co-operate in the investigation of complaints. Care must be taken to ensure that practical arrangements are in place for all relevant US sectors. Existing regulatory agencies, such as the Federal Trade Commission and the Office of the Comptroller of the Currency can perform such a role in the areas for which they have competence.

7. In terms of its substantive content, any acceptable set of "safe harbor" principles must, as a minimum requirement, include all the principles set out in the OECD Privacy Guidelines of 1980, adopted amongst others by the United States and recently re-endorsed at the OECD's Ottawa Conference on Electronic Commerce. These principles are also applied by Directive 95/46/EC as well as by national legislation of the Member States of the European Union. In this regard, the above mentioned consultative text of principles published by the US Department of Commerce on 4 November 1998 raises some concerns, in particular:

   a) The individual's right of access is limited to that which is "reasonable". The OECD Privacy Guidelines do not limit the right itself, simply asserting that it must be exercised "in a reasonable manner".

   b) The purpose specification principle of the OECD Privacy Guidelines is absent, and is only partly replaced by a "choice" principle which in effect allows data collected for one purpose to be used for another, provided individuals have the possibility of opting out.

   c) Proprietary data and any manually processed data are entirely outside of the scope of the US principles, while the "choice" principle provides no

protection to data collected from third parties and the "access" principle excludes public record-derived information.

d) According to the third paragraph of the introduction, “adherence to the principles is subject to” a number of exceptions and limitations such as “risk management” and “information security”. The Working Party takes the view that these notions are too vague and open-ended, and recommends that they be clarified or deleted.

Done at Brussels, 26 January 1999

For the Working Party

The Vice-Chairman

Prof. Stefano RODOTA

ANNEX 2: OPINION 2/99

5047/99/EN/final
WP 19

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

Opinion 2/99 on

the Adequacy of the "International Safe Harbor Principles" issued by the US Department of Commerce on 19th April 1999

Adopted on 3 May 1999

OPINION 2/99 ON

THE ADEQUACY OF the the "International Safe Harbor Principles" issued by the US Department of Commerce on 19th April 1999

The discussions between the European Commission and the United States government have progressed since the Working Party issued its opinion on the level of data protection in the US in January 1999[2]. Recently, the Commission submitted to the Working Party a revised version of the Department of Commerce Principles with a view to obtaining an opinion on the level of data protection they provide.

The Commission has also indicated to the Working Party that it is envisaging the adoption of a decision based on Article 25.6 of the Directive[3] with regard to these Principles, if they are found to provide an adequate level of protection for the transfer of data from the EU to US companies joining the Safe harbor scheme.

The present version of the Principles however cannot be considered final as it contains a number of footnotes indicating areas where a satisfactory understanding with the US has not yet been reached. Hence, the Working Party considers this opinion to be provisional and partial. Provisional insofar as the documents are not final yet and the status of the FAQs (Frequently asked questions) issued by the Department of Commerce has not been clearly indicated to the Working Party (its contents are therefore not taken into account in the present opinion). And partial because the Working Party does not have all the documents necessary for an overall examination of the US situation and namely an overview of the enforcement aspects of the Principles and analysis of the protection awarded by US sectoral laws.

The Working Party reiterates its view that the patchwork of narrowly focused sectoral laws and self-regulatory rules presently existent in the United States cannot be relied upon to provide adequate protection in all cases for personal data transferred from the European Union. It therefore considers the approach of the "Safe Harbour" useful and encourages the Commission to pursue its work towards a finding of a set of principles that the Department of Commerce will issue, thus providing a benchmark for US companies wishing to ensure that they meet the Directive's adequate protection requirement.

The Working Party considers it useful to examine the practical implications of this arrangement on the work of the National Supervisory authorities.

---

2 Opinion 1/99 concerning the level of data protection in the US and the ongoing discussions between the European Commission and the United States government, adopted by the Working Party 26th January 1999

3 A draft Commission decision was circulated to the Working Party on 30th March 1999

On the practical implications of the "Safe Harbour" for the work of the National Supervisory authorities

1. The Working Party considers it very important that US based companies adhering to the "Safe Harbour" Principles be unequivocally identified. Hence the Department of Commerce's recommendation that US companies wishing to join the scheme should notify their intention to the Department of Commerce itself, is indeed very welcome. But it is the Working Party's view that this notification should be as complete as possible, publicly available and should in particular contain an indication of the contact person within the company that is able to deal with requests from the individual and the monitoring body responsible for enforcing the Principles.

2. It is noted that to qualify for the "Safe Harbour" scheme, US organisations may "…join a private sector developed privacy program…." or do so by virtue of US law that effectively protects privacy to the extent that its activities are regulated by such laws. The Working Party seeks further clarification as to the identity of the privacy programs and their operational criteria. As far as the US sectoral laws are concerned, the Working Party also requests further clarification as to their exact content with regard to the protection of privacy.

3. The Working Party also notes that the Safe Harbour Principles only relate to the lawfulness of the international aspect of transfers of data, flowing from Articles 25 and 26 of the Directive. Data exporters based in Europe (whether or not they are affiliates of a US based company adhering to the Safe Harbor) are subject to the application of the other provisions of the directive, e.g. concerning notifications of processing to national supervisory authorities.

4. Moreover, the task of supervisory authorities would be facilitated by a comprehensive description of the powers of the various regulatory authorities. The Working Party has been informed that this document is in preparation by the US authorities.

5. Considering the role of national supervisory authorities in issuing authorisations for international transfers based on contracts, the Working Party seeks clarification on the meaning of the last phrase of paragraph 4 of the introduction, which reads "*Organisations may also put in place the safeguards deemed necessary by the EU for transfers of personal data from the EU to the US by incorporating the relevant safe harbor principles into agreements entered into with parties transferring personal data from the EU*".

6. Finally with regard to the possibility for organisations adhering to the Department of Commerce's principles to rely on National Supervisory authorities for the implementation of the Principles, the Working Party notes that National supervisory authorities do not have jurisdiction in third countries and consequently lack any enforcement powers which would allow them to oversee effectively the implementation of the Principles by US organisations.

On the content of the Principles themselves, the Working Party recognises that in comparison with the 4th November version, although the Principles have been weakened in some aspects, progress has been achieved in many areas. In particular:

- The definition of personal data refers now to an identified or identifiable individual;
- The exceptions to the Principles appear more coherent and in part reflect those envisaged in the directive. This is in particular the case with regard to the deletion of expressions such as "risk management", "information security," and "proprietary data".
- In "Notice" the individual is to be informed of a change of purpose;
- Sensitive information is now fully defined in Principle 2: " Choice";
- Onward transfers now differentiates between transfers amongst organisations adhering to the Principles and transfers to third parties outside the Safe harbor scheme.

The Working Party considers that the standard set by the OECD guidelines of 1980 cannot be waived as it constitutes a minimum requirement for the acceptance of an adequate level of protection in any third country. On the basis of the work previously carried out by the Working Party on the issue of transfer of data to third countries[4], the Department of Commerce 's "Safe Harbor" Principles of 19th April give rise to the following concerns:

1. In the introduction there is reference to the exceptions provided for in Member States' law. The Working Party does not believe this to be appropriate as it could open the door to the interpretation of national implementation measures by organisations adhering to a third country's self-regulatory scheme. Furthermore, it is the Working Party's view that limiting the application of the Safe Harbor Principles to the extent necessary to meet US regulatory provisions, is too wide an exemption, the limits of which are not foreseeable.

2. With regard to manual data, the Working Party considers that there should be equality of treatment for automated and manually processed data held in filing systems. The Working Party therefore endorses the Commission's reserve expressed in the footnotes. But it also believes that organisations adhering to the Safe harbor principles that apply these Principles to manually processed data, if they so wish, should be given the benefits of the "Safe Harbor" for such data collected from Europe.

3. Principles 1 and 2: Notice and Choice:

   Considering that the protection offered by the Safe Harbor Principles pivots around "Notice and Choice", it is paramount that these principles offer comprehensive privacy protection both with regard to the use and the disclosure of the data.

[4] Transfers of personal data to third countries : Applying Articles 25 and 26 of the Data Protection directive, adopted by the Working Party on 24th July 1998

With reference to the "Notice" Principle it is noted that in order for it to be coherent with the "Data security" Principle, the individual should be informed that data is collected only to the extent necessary to fulfil the purposes of collection.

Moreover, the phrase "what type of information" should be re-inserted as it is important that the individual is informed of the type of personal information that is being gathered about him/her.

It should also be explicitly indicated that the individual should receive notice of processing by a US organisation when the data was not provided directly by him/her but was gathered through a third party. This is important in relation to the opportunity to exercise "choice".

The Working Party also seeks clarification as to the exact meaning of the expression "or as soon thereafter practicable", as it considers that the individual should be informed at the time of collection and not at the discretion of each controller.

With regard to the Choice Principle: As noted in the Working Party's previous opinion on the Safe Harbor Principles, the purpose specification principle of the OECD guidelines is absent and only partly replaced by a "Choice" Principle which in effect allows data collected for one purpose to be used for another.

In addition, individuals have the possibility of opting out only if the new purpose is considered incompatible with that given in "Notice". In the Working Party's view, the individual should at least have an opt-out choice in all cases where his data is used for an unrelated purpose and for direct marketing. The standard of consent is higher, for example, when data is collected in a contractual relationship and is subject to express or implied terms of contract.

This is particularly important because, as inevitably in a self-regulatory system, there is no independent determination of what is an incompatible purpose or what are the criteria for establishing that a purpose is incompatible with that given in "Notice".

It is also the Working Party's view that whenever consent is required it should be informed, freely given and unambiguous and that the lack of response from the individual cannot be construed to mean consent.

Finally with regard to the last sentence of the "Choice" Principle, the Working Party seeks clarification as to the exact meaning of the word "or" in the expression "affirmative or explicit (opt in) choice" in the sense of "*affirmative, that is, explicit choice*".

4. Principle 3: Onward transfer – Although not present in OECD guidelines, this principle is necessary to ensure that data is not transferred by a US company that abides by the Safe Harbor Principles to another controller in the US or indeed elsewhere not offering adequate protection. But as presently drafted, it is not clear what the applicable rule is. We understand that the individual should be able to opt out of a transfer to a third party. To this end, he needs at least the information that

data shall be transferred and whether or not the third party adheres to the safe harbor principles or how adequate protection is provided otherwise. The Working Party therefore supports the Commission's request expressed in footnote 5 that explicit notice and choice are to be provided when personal data is transferred to a third party that does not adhere to the Safe Harbor Principles.

5. Principle 6: Access – It is noted that there is no agreement on the text of Principle 6. In the view of the Working Party, Principle 6 should clearly state that the general rule is that access is to be given although some exceptions are possible. These exceptions should be clearly listed in the text of Principle 6. The Directive mentions a number of such exemption in Article 13. An example could be "trade secrets" although participants indicated that at Member States level this problem could never result in the data subject being refused all information. In its contacts with the Department of Commerce, the Commission should be guided by OECD guidelines on this question. The Working Party proposes the following text as a working basis

   "Individuals must have access to information about them that an organisation holds and be able to correct and amend that information where it is inaccurate except where granting access would damage the organisation by the revelation of trade secrets or the non-respect of intellectual property rights or where the burden and cost to the organisation for retrieving the information or other consequences would be clearly disproportionate to the specific risks to the protection of individual's privacy that non-disclosure should entail."

   In addition, the principle should clearly state the data subject's right to get data deleted if the processing of the data is unlawful.
   For the reasons indicated in the introduction, the Working Party did not examine the text of the Frequently Asked questions on Access.

6. Principle 7: Enforcement – It is not sufficiently clear from the text of the Principle itself and that of "Note" of the standard required from companies. In the Working Party's view, data protection rules only contribute to the protection of individuals to the extent to which they are followed in practice. In an entirely voluntary scheme such as this compliance with the rules must be at least guaranteed by an independent investigation mechanism for complaints and sanctions which must be, on the one hand dissuasive and, on the other hand give individuals compensation, where appropriate. The present text of the Principle 7 implies that compensation will be provided only where the "applicable law and private-sector initiatives so provide". Besides, the Working Party fully endorses the Commission's request to see all conditions listed in Principle 7 met before a company can be deemed to comply with the Safe harbor principles.

   In addition, Principle 7 does not establish the rules to be followed for the verification of compliance nor does it indicate which authorities can enforce the Principles. Similarly, it should be indicated what type of sanctions are envisaged, who determines them and according to which procedure.

   As indicated in the introduction, with regard to the co-operation between National Supervisory authorities and US based organisations wishing to join in the "Safe

Harbor", the Working Party does not consider it feasible to rely on National Supervisory authorities for the implementation of the Principles. However if enforcement is ensured in the US by independent monitoring bodies, then co-operation between such bodies and the National supervisory authorities on a case by case basis, could be envisaged.

Conclusions

On the basis of the above, the Working Party encourages the Commission to pursue its efforts in the dialogue with the Department of Commerce with a view to reinforce the protection afforded in the" International Safe Harbor Principles".

In particular, the Working Party invites the Commission to take into account the issues raised and keep the Working Party informed of its contacts with the US Department of Commerce.

Done at Brussels, 3 May 1999

For the Working Party

The Chairman

P.J. HUSTINX

ANNEX 3: OPINION 4/99

5066/99/EN/final
WP 21

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

Opinion 4/99 on

The Frequently Asked Questions to be issued by the US Department of Commerce in relation to the proposed "Safe Harbor Principles"

Adopted on 7 June 1999

Opinion 4/99 on
the Frequently Asked Questions to be issued by the US Department of Commerce

In its Opinion 2/99[5], adopted on 3 May 1999 and concerning the "International Safe Harbor Principles" (hereinafter: "the principles"), the Working Party had not taken into account the Frequently Asked Questions issued by the US Department of Commerce on 30 April 1999 (hereinafter: "the FAQs"). Before expressing its views on the content of the FAQs, the Working Party had requested that the status of the FAQs be clarified.

On 2 June 1999, DG XV copied to the Working Party[6] the letter sent to the members of the Committee established by Article 31 of Directive 95/46/EC and the attached set of documents: in particular, a revised and confidential version of the Safe Harbor Principles and a list of FAQs, six of which are attached to the list[7].

Having examined the above referred letter, the Working Party understands that it is the intention of the US side to issue the FAQs as authoritative guidance to the principles, and that this should be reflected in the final version of the Article 25(6) Decision.

The Working Party agrees that this solution would be desirable for two reasons: on the one hand, it would allow to clarify and, in some cases, to complete the principles in relation to certain categories of processing operations, and this would be helpful in assessing the principles themselves; on the other, the authoritative guidance would help the complaints bodies in the interpretation and application of the principles to the concrete cases. However, this requires that before taking a decision on the adequacy of the principles, due consideration should be given to each and every FAQ. The Working Party takes the view that such thorough consideration is required by Article 25(2) of the Directive, according to which "the adequacy of data protection shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations".

The Working Party notes that a list of FAQs has now been established and that the list includes fifteen FAQs. The Working Party notes that, if compared to the nine FAQs circulated in April and May, the list includes six new FAQs[8]. The Working Party also notes that, if compared to the previous version, a number of changes have been introduced in the FAQs attached to the letter of DG XV.

---

[5] Opinion 2/99 on the Adequacy of the "International Safe Harbor Principles" issued by the US Department of Commerce on 19th April 1999, adopted on 3 May 1999, available at: http://www.europa.eu.int/comm/dg15/en/media/dataprot/index.htm

[6] Established by article 29 of 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, JO L 281, 23 November 1995, p. 31. Available at: see footnote 1.

[7] See annex 1: List of FAQs. See annex 2: Frequently Asked Questions, n° 1 to 6, version 1 June 1999.

[8] The text on these six new FAQs was not available on 3 June.

The Working Party considers that a reasonable delay is indispensable to carry out a meaningful assessment of the FAQs, as requested by Article 25 of the Directive. In particular, such a delay should allow the appropriate internal consultations at the national level with a view to the procedure laid down in Article 31 of the Directive. This Opinion is therefore intended to provide only a preliminary view on the possible status of the FAQs as well as on the FAQs circulated on 2 June 1999. This is without prejudice to the comments that the Working Party intends to make on the new version of the principles and on the FAQs that remain to be circulated, nor to the global assessment of the "safe harbor" approach, since other elements of the package will need to be considered (e.g.: the draft exchange of letters).

I. Status of the FAQs

On the basis of the above, the Working Party takes the view that:

1. the Frequently Asked Questions (FAQs) listed in the Annex, when issued by the US Department of Commerce, should have authoritative status provided that they are consistent with, and are considered together with, the Safe Harbor Principles;
2. a thorough assessment of all the FAQs, within a reasonable delay involving internal consultation, needs to be undertaken before deciding whether the Safe Harbor Principles would provide an adequate level of protection;
3. the Decision that may be taken in relation to the principles should contain a reference to the FAQs;
4. the final list of FAQs should be exhaustive and no change to the FAQs should be introduced unilaterally. However, the FAQs should be looked at in the light of experience in any review of the implementation of the Safe Harbor arrangement and may need to be adapted and/or supplemented.

II. List of FAQs

The Working Party welcomes the principle of enlarging the list of FAQs and considers that, due to the lack of clarity of some of the principles, the FAQs ought to provide clear, unambiguous and authoritative guidance to data controllers as well as the necessary guarantees to the individuals concerned. The Working Party wishes to see the remaining texts of draft FAQs as soon as possible and attaches importance in particular to :

1. "**independent investigation of complaints**" **(FAQ N°11).** Given that no improvements have been made to the "enforcement" principle, and in the absence of equivalent guarantees, the Working Party confirms that the credibility of the Safe Harbor as a whole depends very much on a satisfactory answer to this element of the enforcement principle;

2. "**opt-out choice**" **(FAQ N° 13).** According to the "choice" principle, opt-out would be offered only where the "use or disclosure is incompatible with the purpose for which it [personal information] was originally collected or with any other purpose or disclosure identified in a notice to the individual". In its opinion

2/99, the Working Party has already stated and motivated its objections to such a narrow notion of "choice" and had made some suggestions for improvement. The best way to achieve this objective remains an improvement of the principle, by taking into accoung the suggestions made earlier in Opinion 2/99, which would mean introducing at least an unconditional opt-out for direct marketing.

III. Sensitive Data (FAQ N° 1)

The Working Party reiterates its view, expressed in Opinion 2/99, that the Safe Harbor Principles only relate to the lawfulness of the international aspects of transfers of data (Articles 25 and 26 of the Directive). The Working Party recalls that data controllers established in the EU (whether or not they are affiliates of US organisations adhering to the Safe Harbor) are subject to the national provisions implementing the other provisions of the Directive, namely those concerning the lawfulness of processing (Articles 6 and 7) and the additional requirements concerning sensitive data (Article 8). The same applies where personal data are collected by US organisations directly from individuals in the EU. The Working Party underlines that, to avoid misleading effects, the FAQ should include the above points.
In particular, it should be recalled that Member States may provide that the prohibition to process sensitive data may not be lifted by the data subject's giving his/her consent (Art. 8 paragraph 2a of the Directive) and that prior notification to the Supervisory Authority may be required.

IV. Journalistic exceptions (FAQ N° 2)

The Working Party attaches the greatest importance to the freedom of press and considers that the Directive strikes the right balance in requiring that Member States provide for exemptions and derogations (article 9). However, such exemptions concern only Chapters III, IV and VI and do not apply to the other provisions of the Directive, such as security of processing (Article 17). The Working Party underlines that its understanding is that the FAQ applies to processing exclusively for journalistic purposes covered by the first Amendment and that the security principle, far from conflicting with the freedom of press, is designed to serve the journalists' interests as well (in particular, to protect their sources and their work against unauthorised access or disclosure, accidental or unlawful loss or alteration, especially where the processing involves the transmission of data over a network). The Working Party therefore considers that there is no reason to derogate from the security principle as defined in the Safe Harbor.

V. Secondary liability (FAQ No 3)

The Working Party sees no difficulty with this text provided that it is construed narrowly and applies only to the situation described in the question.

VI. Headhunters etc. (FAQ N° 4)

In its Opinion 2/99, the Working Party had already reaffirmed that the standard set by the OECD guidelines of 1980 could not be waived as it constitutes a minimum requirement for the acceptance of an adequate level of protection.
The Working Party notes that the FAQ introduces exceptions not mentioned in the principles themselves. It would need to be explained which processing operations are covered by each of the exemptions mentioned and why they are limitative in character. Moreover, it should be made clearer for which principles (notice, choice) the legitimate interest of the organisation and the public interest requirement provides exemptions. Finally, the legitimacy of the activity of a headhunter or an investment banker would seem to depend on other factors not mentioned.

VII. The role of Data Protection authorities (FAQ No 5)

The Working Party welcomes the clarification provided by this FAQ and would wish to give further positive consideration to this matter, especially as regards the role the National Data Protection Authorities might play in complaint handling. A number of questions, however, require more detailed examination, in particular :

- how the option will be exercised, what will determine the identity of the « relevant data protection authority » and whether this will still be subject to the agreement of the authority concerned ;
- for some authorities, the compatibility of this role with their statutory powers and duties, as established and limited by national law ;
- the impact on resources.

If this examination confirms that the authorities can play a constructive role, the Working Party sees a need for :

- the possible closer definition of the cases in which their direct involvement might be an appropriate and practicable solution ;
- a clear understanding about the follow-up action required in cases where a US organisation does not fulfil its commitment to cooperate with the data protection authority.

The Working Party emphasises in any case the importance of ensuring that all three elements of principle 7 (dispute resolution and remedies, verification and sanctions) are guaranteed for all participants in the Safe Harbor, whatever the mechanisms chosen, as well as procedures which are accessible and easy to follow for data subjects.

VIII. Self-certification (FAQ N° 6)

The Working Party confirms its concern that self-certification may lead to abuses. As a minimum, the Working Party considers that, in case of misrepresentation concerning the qualification criteria (e.g. where an organisation does not meet the requirements of Principle 7) the "impostor" is taken out of the list. The same should apply where US-based organisations having adhered to the Safe Harbor arrangements with a commitment to cooperate with an European Data Protection Authority, do not fully honour this commitment.

Done at Brussels, 7 June 1999

For the Working Party

The Chairman

P.J. HUSTINX

ANNEX 1 : LIST of FAQs, version 1 June 1999

LIST OF THE FAQs RELATING TO THE US SAFE HARBOR PRINCIPLES

1) SENSITIVE DATA
2) JOURNALISTIC EXCEPTIONS
3) SECONDARY LIABILITY
4) HEADHUNTERS
5) THE ROLE OF DATA PROTECTION AUTHORITIES
6) SELF-CERTIFICATION
7) VERIFICATION
8) ACCESS
9) HUMAN RESOURCES DATA
10) ARTICLE 17 CONTRACTS
11) INDEPENDENT INVESTIGATION OF COMPLAINTS
12) RISK MANAGEMENT
13) OPT- OUT CHOICE
14) AIRLINE PASSENGER RESERVATIONS
15) PHARMACEUTICALS

ANNEX 2 : TEXT of FAQs N° 1 to 6, version 1 June 1999

Frequently Asked Questions (FAQs)

FAQ N° 1 - Sensitive Data – 31st May 1999

Q: Must an organization always provide explicit (opt in) choice with respect to sensitive data?

A: No, such choice is not required where the processing is: (1) in the vital interests of the data subject or another person; (2) necessary for the establishment of legal claims or defenses; (3) required to provide medical care of diagnosis; (4) carried out in the course of legitimate activities by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to the persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; (5) necessary to carry out the organization's obligations in the field of employment law; or (6) related to data that are manifestly made public by the individual or is necessary for the exercise or defense of legal claims.

FAQ N° 2 - Journalistic Exceptions – 31ST May 1999

Q*: Given U.S. constitutional protections for freedom of the press and the Directive's exemption for journalistic material, do the safe harbor principles apply to personal information gathered, maintained, or disseminated for journalistic purposes?*

A: Where the rights of a free press embodied in the First Amendment of the United States Constitution intersect with privacy protection interests, the First Amendment must govern the balancing of these interests with regard to the activities of U.S. persons or organizations. Information that is gathered for publication, broadcast, or other forms of public communication of journalistic material, whether used or not, as well as information found in previously published material disseminated from media archives, is not subject to the requirements of the safe harbor principles.

FAQ N° 3 - Secondary Liability - 31st May 1999

Q: Are ISPs, telecommunications carriers , or other organizations liable under the safe harbor principles when on behalf of another organization they merely

transmit, route, switch, or cache information that may violate their terms?

A: No. As is the case with the Directive itself, the safe harbor does not create secondary liability. Where an organization is acting as a conduit for the data and does not determine the purposes and means of processing the personal data, it would not be liable.

FAQ N° 4 – Headhunters, Investment Banking and audits – 30th April 1999

Q: Some business activities necessarily involve processing personal data without the knowledge of the individual, for example, the activities of headhunters, investment bankers, and auditors. Is this permitted by the Safe harbor principles?

A: Yes. As it is the case with the Directive itself, the safe harbor does not create unqualified requirements to seek the consent of the individual, to inform individuals that their data is being processed, or to give individuals access to their data. Exceptions are permitted, for example, where the public interest requires or when processing is necessary for legitimate interests pursued by the organisations or third parties to whom data are disclosed, except to the extent where the individual's privacy rights override such interests. The activities of headhunters, investment bankers, and auditors are legittimate interests.

FAQ N° 5 – The role of Data Protection authorities [9]

Q: How will companies that commit to cooperate with European Data Protection Authorities make those commitments and how will they be implemented?

A: Under the safe harbor, US organizations receiving personal data from the EU must commit to employ effective mechanisms for assuring compliance with the safe harbor principles. More specifically, they must provide (1) recourse for individuals to whom the data relate, (2) follow up procedures for verifying that the attestations and assertions they have made about their privacy practices are true, and (3) obligations to remedy problems arising out of failure to comply with the principles and consequences for such organizations. The enforcement principle allows organizations to make a commitment to cooperate with the data protection authorities ("DPAs") in the European Union as one means of satisfying the enforcement principle under the safe harbor. Organizations electing this option would have to follow the notification procedure and other requirements set forth below.

NOTIFICATION PROCEDURE

An organization may commit to cooperate with the DPAs by declaring in its

[9] Text distributed to participants during the last meeting of the Article 31 Committee on 21st May. This text will become an FAQ if National Data Protection Authorities agree to fulfil this role.

safe harbor notification to the Department of Commerce that the organization:

> (1) elects to satisfy (a) and (c) of the safe harbor enforcement principle by committing to cooperate with the relevant DPA(s);
>
> (2) will cooperate with the relevant DPA(s) in the investigation and resolution of complaints brought under the safe harbor; and
>
> (3) consistently with the Article 25.6 Decisions and the [Draft Paper on EU Procedures], will comply with any decisions of the DPA where the DPA determines that the organization must take additional steps to comply with the safe harbor principles, including remedial or compensatory measures for the benefit of individuals affected by noncompliance with the principles, and consequences for the organization.

HOW IT WOULD WORK

In safe harbor situations where the US organization had elected to cooperate with data protection authorities, European consumers, employees, or other affected individuals, after raising an issue or complaint with the US organization, would raise unresolved issues with the relevant DPA. The DPA would then turn to the US importing organization with any questions it had about the complaint. Where complaints or other specific concerns lead the DPA to investigate further, the US organization is committed, under its safe harbor notice to the Department of Commerce, to cooperate with the DPA.

This would mean, for example, that the US organization would have to respond to inquiries from and otherwise make itself available to the DPA, furnish information or stored data upon the DPA's request, report on security measures, or provide the DPA with remote or physical access to data banks and other data facilities. The US organization would provide requested information to the DPA(s) in Europe. DPAs would not be required to travel to the US to investigate complaints.

Where the parties themselves agreed to steps for resolving the complaint, such as removing an individual from a mailing list or correcting or suppressing certain data, the US organization, pursuant to its cooperation commitment, would be obligated to give effect to such an agreement with respect to relevant data stored in the United States. If the parties are unable to agree on whether there is compliance with the safe harbor principles or on the remedial or compensatory measures to be taken by the US companies, the DPA would take a decision. Again, the US organization would be bound by its public commitment to abide by the results of these procedures, subject to the review procedures set forth in the Draft Paper on EU Procedures.

These results are essentially the same that would obtain in the case of a US organization that failed to abide by the decisions of a relevant self-regulatory body. The difference here is that the investigation and determination of compliance and remedies would be made in the first instance by the DPA without resort first to recourse mechanisms offered by a self-regulatory body in the United States.

This should not be unduly burdensome for DPAs. Absent this enforcement option under the safe harbor, DPAs would be obliged in any event to investigate and take decisions on complaints arising from data transfers to the United States, but such enforcement would take place later in the complaint process set forth in the [Draft Paper on EU Procedures].

RATIONALE

The option of committing to cooperate with DPAs is an important enforcement alternative for US organizations for a number of reasons. First, recourse to private sector complaint resolution in the US is not an ideal way to resolve data protection issues arising out of employment relationships based in Europe. Cooperating with DPAs would be a far better alternative for this type of complaints. Second, this enforcement option could allow US organizations to qualify for the safe harbor more quickly than if they have to rely on US developed self regulatory mechanisms. It is unlikely that self regulatory mechanisms will be available for all categories of data transfer to the US as soon as the safe harbor goes into effect. While some private sector programs are in development, complete development and implementation of these and other programs will undoubtedly lag until closure of the safe harbor discussions. Committing to cooperate with DPAs can help to fill this gap. Finally, this option would allow more US organizations to participate in the safe harbor. Some US organizations, either because their business is relatively unique or for other reasons, may find it difficult to find self regulatory organizations able to address their particular needs. And, there may be no US statutory or regulatory agency authorized to hear such complaints. Committing to cooperate with DPAs would allow these organizations nonetheless to qualify for the safe harbor.

FAQ N° 6 - Self-Certification – 31st May 1999[10]

Q: How does an organization self-certify that it adheres to the safe harbor principles?

A: To self-certify for the safe harbor, organizations will need to provide to the Department of Commerce, or its designee, a letter, signed by a corporate officer, that contains at least the following information:

name of organization, mailing address, email address, telephone and fax numbers;
description of the main activities of the organization;
description of the organization's privacy policy, including -- where it is available for viewing by the public,
-- its effective date of implementation
-- a contact person for the handling of complaints, access requests, and any other issues arising under the safe harbor,

[10] As the Self-certification FAQ describes the information companies have to provide to the DoC in order to be inserted in the "Safe harbor register", this text should no longer be an FAQ but should be annexed to the Safe harbor principles themselves. The US side is ready to agree to this, if they get satisfaction on the status of the FAQs.

-- the specific statutory bodies that have jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices,

-- name of any privacy programs in which the organization is a member,

-- method of verification (e.g. in-house, third party)*, and

-- [] independent recourse mechanism that/ is available to investigate unresolved complaints.

The Department (or its designee) will maintain a list of all organizations that self-certify for the safe harbor. Both the list and the self-certification letters submitted by the organizations will be made publicly available. All organizations that self certify for the safe harbor must also state in their published privacy policy statements that they adhere to the safe harbor principles. Any misrepresentation to the Department or to the general public concerning an organization's adherence to the safe harbor principles may be actionable by the Federal Trade Commission or other relevant statutory body.

*See FAQ on verification