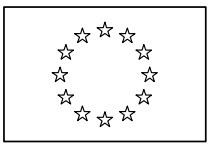

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 20.10.2004
SEC (2004) 1323

COMMISSION STAFF WORKING DOCUMENT

The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce

TABLE OF CONTENTS

I. INTRODUCTION

1. Background

Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter "data protection Directive") restricts transfers of personal data from EU Member States to other countries outside the EU where the legal regime does not ensure an adequate level of privacy protection for natural persons[1].

The Commission may find that a third country ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into with the Commission in order to protect privacy rights of individuals in which case the restriction on data transfers to a such country would not apply[2]. In the context of this competence, and further to a fruitful transatlantic dialogue, on 26 July 2000, the Commission adopted Decision 520/2000/EC[3] ("Safe Harbour decision") recognizing the Safe Harbour Privacy Principles and Frequently Asked Questions (respectively "the Principles" and "FAQs"), issued by the Department of Commerce of the United States, as providing adequate protection for the purposes of personal data transfers from the EU[4]. As a result, data transfers from EU Member States[5] to the US organisations that subscribe to the Principles can take place lawfully insofar as the recipient organisations are deemed to provide an adequate level of privacy protection[6].

The Safe Harbour decision establishes that the Commission will make an assessment of its implementation three years after its notification to the Member States and report its findings to the Committee established under Article 31 of the data protection Directive[7]. This should include any evidence that could affect the evaluation whether the Principles and FAQs provide adequate protection as well as any evidence that the decision is being implemented in

---

1 Articles 25 and 26 of the data protection Directive set forth the legal framework for transfers of personal data from the EU to third countries outside the EEA.

2 These decisions are commonly referred to as "adequacy decisions".

3 Commission decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce in OJ 215 of 28 August 2000, page 7.

4 To facilitate the understanding of this report, this footnote contains an overview of the main aspects of the Safe Harbour. To take advantage of the Safe Harbour, a US organisation must decide voluntarily to rely on the Principles and FAQs, bring itself into compliance with the Principles and FAQs, identify in its publicly available privacy policy that it adheres to the Principles and declare to the US Department of Commerce that it is in compliance with the Principles. For an overview of the content of the Principles, see Section II, point 2 entitled "Incorporation of the Safe Harbour Privacy Principles in privacy policies". Failure to abide by the Principles must be actionable under law or statute as an unfair or deceptive act. The competent bodies for enforcing the Principles are the Federal Trade Commission and Department of Transportation. US law applies to question of interpretation and compliance with the Principles by organisations that self-certified, except where organisations have committed themselves to cooperate with European data protection authorities.

5 Data transfers from the three States Parties to the EEA are similarly affected, following extension of Directive 95/46/EC to the EEA Agreement, Decision 38/1999 of 25 June 1999, OJ L 296/41, 23.11.2000

6 The above does not exclude the application to the data processing of other requirements that may exist under national data protection legislation.

7 The Committee established under Article 31 is a committee composed by representatives of the Member States. The Commission must seek an opinion of this Committee before adopting an adequacy decision.

a discriminatory way[8]. The present report aims to comply with this obligation. This report also seeks to honour Commissioner Bolkestein's undertaking, following the Parliament's resolution of 5 July 2000, to make periodic reports to the Working Party 29[9] and to the relevant committee of the European Parliament on the operation of the Safe Harbour. The present report was preceded by the "Commission Staff Working Paper" adopted in February 2002, which gave a first assessment of the functioning of the Safe Harbour decision[10].

2. Objective and methodology

In order to assess the implementation of the Safe Harbour decision, this report looks into the following issues. First, it identifies trends in the compliance of registered US organisations with certification rules and with the terms of the Safe Harbour privacy Principles and related FAQs. Second, it examines whether the elements to support the implementation of the Principles and FAQs work in practice. In particular, it looks into whether the US Department of Commerce (hereinafter "US DoC"), as the body responsible for handling organisations' certification to the Safe Harbour Principles, carries out its role properly. In that context, the report also assesses whether the bodies involved in the hearing of complaints from individuals and for enforcing the Principles are carrying out their functions properly. Under this category, the following bodies are included: Federal Trade Commission (hereinafter "FTC")[11], alternative dispute resolution mechanisms (hereinafter "ADRs"), and the panel of EU data protection authorities (hereinafter "EU panel"). Finally, it ascertains whether the decision is being implemented in a discriminatory manner.

The report is based both on the Commission services' experience and on a study on the implementation of the Safe Harbour which the Commission services assigned to a third party contractor, a group of Universities specialising on data protection issues[12]. Among others, the material evaluated includes the following: (i) US DoC certification page, including all the letters of organisations self certifying their adherence to the Principles; (ii) privacy policies of

---

8 Article 4 of […]: "1. This Decision may be adapted at any time in the light of experience with its implementation and/or if the level of protection provided by the Principles and the FAQs is overtaken by the requirements of US legislation. The Commission shall in any case evaluate the implementation […] on the basis of available information three years after its notification […] and report the findings to the Committee […] including any evidence that could affect the evaluation that the provisions set out in Article 1 […] provide adequate protection […] and any evidence that the present Decision is being implemented in a discriminatory way. 2. The Commission shall, if necessary present draft measures in accordance with the procedure referred to in Article 31 of Directive 95/46".

9 Working Party 29 formally, Working Party on the protection of individuals with regard to the processing of private data, is a body, among others, competent for interpreting the provisions of the data protection Directive. It carries out this task by issuing recommendations, opinions and working documents on different aspects of the data protection Directive. Working Party 29 is composed of representatives of national data protection authorities of the EU Member States.

10 Commission Staff Working Paper entitled "The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce". Brussels 13.02.2002, SEC (2002) 196.

11 Because all but one organisation that have self certified to the Principles falls within the jurisdiction of the FTC, for the purposes of this report we will focus on the FTC as enforcement body.

12 The study, entitled "Safe Harbour Agreement Implementation Study" was carried out by Professor Dr. Y. Poullet, J. Dhont and M.V. Perez Asinary from the Centre de Recherches Informatique et Droit (University of Namur, Belgium) with the assistance of Dr. Bygrave (University of Oslo, Norway) and Dr. Reidenberg (Fortham University School of Law, US). The report will soon be available at the Commission's web site: http://europa.eu.int/comm/internal_market/privacy/index_en.htm.

10 percent of the organisations that self-certified to the Principles; (iii) privacy policies of eight independent dispute resolution mechanisms[13]. The Commission/contractor has received feedback from, among others, the following bodies/organisations: (i) private organisations that subscribe to the Principles; (ii) public US and EU organisations such as US DoC, FTC, and data protection authorities; (iii) private organisations that provide dispute resolution mechanisms; and (iv) EU consumer associations[14].

In the implementation of the recommendations made in this report, the Commission services hope to see a continuation of the open dialogue and constructive cooperation with the DoC and FTC that has been maintained throughout the preparation of this report. In this regard, the Commission services welcome the DoC's eagerness to work with the Commission and the EU panel towards addressing the shortcomings in the implementation of the Safe Harbour identified in the preparation of this report.

3. The Safe Harbour in numbers

At the end of 2003, the number of companies that had self-certified to the Safe Harbour was over 400[15]. The Commission is pleased to see that since the adoption of the Safe Harbour decision, the number of organisations that have subscribed to the Safe Harbour has constantly increased. 158 organisations were added to the Safe Harbour List in 2002 and 156 in 2003. This continuous and steady growth is welcome. Without this growth in the Safe Harbour's membership, it is uncertain whether the transfer of personal data from EU-based data controllers to these organisations would have been subject to adequate protection.

However, the number of registered organisations is lower than initially anticipated and this is a cause of disappointment for the Commission services insofar as the benefits of the Safe Harbour would be greater (both for companies and for data subjects) if membership were to increase further. If the recommendations made in this report are properly implemented by the different organisations involved in the Safe Harbour, the Commission services hope that it will foster awareness regarding the Safe Harbour scheme which ultimately may increase the number of organizations that certify to it.

In the preparation of future reports, the Commission may consider analysing the market share of the organisations that subscribe to the Safe Harbour or at least the market share of a specific sector (i.e., direct marketing). Such analysis will provide an accurate indication of the Safe Harbour level of membership, at least in a specific sector. Such analysis will have to take into account that certain sectors such as financial services are not Safe Harbour eligible.

---

13 The companies analyzed under (ii) were selected randomly. The privacy programs and independent dispute resolution mechanisms correspond to those mentioned by the 10 percent of the organisation analysed under (ii).

14 The analysis was carried out mainly between November 2003 and March 2004. The publicly available material, namely the privacy policies of companies and of dispute resolution mechanisms were printed between November 2003 and February 2004.

15 401 companies were listed on the Department of Commerce Certification page on 3 November 2003

II. ASSESSMENT OF US ORGANISATIONS' COMPLIANCE WITH THE SAFE HARBOUR PRINCIPLES

A US organisation that wants to join the Safe Harbour must: (a) identify in its publicly available privacy policy that it adheres to the Principles and actually does comply with the Principles, as well as (b) self-certify i.e., declare to the US Department of Commerce that it is in compliance with the Principles[16].

Evaluating US organisations' compliance with the Safe Harbour can be undertaken in several ways. One way is by performing an audit to check the organisations' actual behaviour i.e., whether they comply with the Principles. Because performing audits is highly resource- and time-consuming and the European Commission has no power to force companies to submit to such audits (which would reveal business confidential and sensitive information), no US organisations have been audited. However, the Commission services note the absence of complaints from data subjects regarding non-compliance which may give some indication of compliance with the Principles. Another way of assessing organisations' compliance with the Safe Harbour consists in analysing companies' publicly available privacy policies. The reason why undertaking such analysis is appropriate is twofold: First, lack of a public self-statement in itself means that Safe Harbour participants are falling short of what the decision requires. Second, to comply with the Safe Harbour, a company must be subject to enforcement actions by the FTC. The FTC's authority to enforce the Principles upon a given organisation is triggered by such an organisation's public commitment to comply with the Principles[17]. Without such a public commitment, the FTC would not have the authority to enforce the Principles. This basically puts the company that lacks a publicly available privacy policy that fully embraces the Principles in non-compliance.

In accordance with the above, in the following sub-section we will describe whether the organisations analysed made publicly available privacy policy declarations and, if so, whether such privacy policies conformed to the Principles.

1. Visibility of the statement of adherence to Safe Harbour Principles

For some of the organisations analysed, no public statement of adherence to the Safe Harbour Principles could be found. For some of the organisations, the privacy policy covered only part of the data processing indicated on the DoC certification page.[18] A small number of organisations did not disclose the privacy policy on the web but ensured that it was available on the intranet. According to the information available to the Commission services, it is unknown whether such policies were indeed available on those organisations' intranet.

While a majority of organisations do comply with the requirement of having a visible privacy policy, a substantial minority do not. For the reasons explained above, this is a key requirement of the Safe Harbour and its not being fully respected is a matter of concern and needs to be corrected.

---

16 AQ 6 requires that "All organizations that self-certify for the Safe Harbour must […] state in their relevant published privacy policy statements that they adhere to the Safe Harbour Principles".

17 Section 5 of the Federal Trade Commission Act prohibiting unfair and deceptive acts.

18 See study "Safe Harbour Agreement Implementation Study" available at the Commission's web site: http://europa.eu.int/comm/internal_market/privacy/index_en.htm.

The Commission services believe the DoC should act to reverse this trend by providing guidelines or best practices on how to draft privacy policies and by endeavouring to ensure that organisations that self-certify to the Principles have a privacy policy publicly available before putting these companies on the Safe Harbour List. Availability limited to in-house arrangements such as employee manuals or intranets is not in conformity with Safe Harbour requirements. Moreover, the Commission services believe that the DoC should consider carrying out periodic checks of websites subsequent to its initial verification procedure to ensure that the privacy policy declarations remain publicly available.

2. Incorporation of the Safe Harbour Privacy Principles in privacy policies

While US organisations seem to make efforts to incorporate the Safe Harbour Principles into their privacy policies, as a general observation, a relevant number of the reviewed US organizations seem to have difficulties in correctly translating the Safe Harbour principles into their data processing policies. This section focuses on those Principles which seem to cause the most problems to US organisations.

Pursuant to the **notice Principle**, organisations must provide notice to data subjects about the collection of data, its purposes and intended transfers (if any). The Commission services' research shows that a number of privacy policies do not describe the processing operations sufficiently and clearly. In addition, sometimes the processing operations are described in different privacy policies, making it difficult for an average individual to know which policy applies. The research further shows a trend followed by a number of companies consisting in not describing the purposes for which personal data is collected and processed. Those which do describe the purposes, often do it insufficiently and ambiguously[19]. Finally, the policies tend to use terminology that is either contrary to the Safe Harbour decision or is not clearly defined, thereby rendering it difficult to understand and ascertain how personal information is actually used. The overall effect is that individuals may not know what rules apply to the processing of their personal data.

According to the **Principle of choice**, organisations must provide individuals with the possibility to opt out of disclosure of their personal data to third parties. Choice is crucial for data subjects to have minimal control as regards the processing of personal data pertaining to them. The Commission services have noted that a number of companies do not give individuals the choice of whether to disclose their personal data to third parties. Where companies did provide such a choice, it was often not done in a clear manner.

Pursuant to the **access Principle**, organisations must ensure that individuals have access on a reasonable basis to all information that might be held about them, including their right to amend or delete any information that is inaccurate. However, the Commission services' research shows that a significant number of companies' policies do not provide for this. In these cases individuals are therefore not informed about how to exercise a significant privacy right, thus undermining their ability to exercise the access right.

Regarding the **enforcement Principle**, which requires companies to identify either an Alternative Dispute Resolution body or the EU panel to hear individuals' complaints, the Commission notes that a number of companies fail to do so. When companies select the EU

[19] See study "Safe Harbour Agreement Implementation Study" available at the Commission's web site: http://europa.eu.int/comm/internal_market/privacy/index_en.htm.

panel, almost all of them fail to state their commitment to comply with the advice of the EU panel as required by FAQ 9, or to indicate how the EU panel can be contacted. When companies select ADRs, they often fail to inform individuals of the arrangements for taking up complaints with the ADR.

The Commission services are concerned that relatively few organisations published privacy policies that reflect all seven Safe Harbour Principles and believe that this problem must be overcome. The Commission believes that it is of the utmost importance to ensure that businesses are aware of the Principles and that they undertake to respect them in their publicly available privacy policy. Individuals thus know what their rights are and how to exercise them. With this in mind, the Commission services propose the following actions to be taken:

First, in contacts with their US counterparts, the Commission's services will highlight the need for a rigorous respect of the Safe Harbour Principles. Companies must be clear about their commitment to the Principles and must comply with them.

Second, the Commission services consider that the DoC should be more proactive with regard to access to the Safe Harbour and to awareness of the Principles. The DoC should take concrete action in order to ensure that the adherent companies have a publicly available privacy policy when they self-certify. The Commission services have brought this issue to the attention of the DoC. The DoC should also ensure that adherent companies which choose to cooperate with European DPAs as their Dispute Resolution method should represent their commitment to comply with DPA decisions when they self-certify.

The Commission services also believe that providing more and better guidance to companies on the mechanisms and Principles would raise the awareness of the Principles. In this regard, the Commission services suggest that the DoC, in cooperation with the EU panel, should provide guidelines or best practices on how to draft privacy policies in accordance with the Principles.

Third, as further highlighted below, the Commission services consider it is essential for the FTC to be more proactive in monitoring organisations' compliance with the Principles and launching investigations where questions exist regarding Safe Harbour compliance. The Commission would like the FTC to apply the same assiduousness to privacy issues related to the Safe Harbour as it has applied to spam related matters, where the FTC has made great efforts in consciousness raising, informing consumers and bringing actions against alleged spammers.

Finally, the Commission thinks that the EU panel and data protection authorities should invite organizations that subscribe to the Principles to effectively comply with the Principles and use their powers to suspend data flows if they conclude that there is a substantial likelihood that the principles are being violated[20].

---

20 The competence to suspend data flows if there is substantial likelihood that the Principles are being violated applies where (i) there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; (ii) the continuing transfer would create an imminent risk of grave harm to data subjects and (iii) the competent authorities in the Member States have made reasonable efforts under the circumstances to provide the organisation with notice an opportunity to respond, (Article 3 of the Commission decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions).

III. ASSESSMENT OF THE FUNCTIONING OF THE UNITED STATES DEPARTMENT OF COMMERCE AS THE BODY RESPONSIBLE FOR HANDLING ORGANISATIONS' CERTIFICATION TO THE SAFE HARBOUR PRINCIPLES

According to FAQ 6, the DoC is under an obligation to maintain a list of all organisations that filed self-certification letters and to make both the list of organisations and the self-certification letters publicly available. FAQ 6 specifies the information that must be contained in the self-certification letter, which organisations can send both on-line and by regular mail[21.] Where organisations wish to self-certify compliance with the Principles regarding human resources data, they must indicate in the self-certification letter their commitment to cooperate with the EU panel and to comply with the advice given by such authorities.

In compliance with FAQ 6, the US DoC has set up a space on its web site (http://www.export.gov/safeHarbour/index.html) dedicated to the Safe Harbour. In addition to featuring the list of organisations that have self-certified to the Principles and the mandatory content of the letters, the DoC web site provides extensive material on the rules that must be followed by organisations that wish to self-certify. Particularly useful is the section that contains an updated compliance checklist for companies to consider before subscribing to the Principles. Also practical is a workbook intended to aid U.S. businesses in assessing their privacy policies and practices with respect to complying with the Principles. However, the DoC's compliance with the legal requirements and particularly with FAQ 6 does not necessarily mean that there is no room for improvement. In this regard, the Commission services have asked the DoC to carry out some changes to its web site, some of a technical nature, which would have the ultimate effect of improving the functioning of the Safe Harbour as a whole[22].

---

21 To self-certify for the Safe Harbour, organisations can provide to the DoC a letter, signed by a corporate officer on behalf of the organisation that is joining the Safe Harbour, that contains at least the following information: 1. name of organisation, mailing address, e-mail address, telephone and fax numbers; 2. description of the activities of the organisation with respect to personal information received from the EU; and 3. description of the organisation's privacy policy for such personal information, including: (a) where the privacy policy is available for viewing by the public, (b) its effective date of implementation, (c) a contact office for the handling of complaints, access requests, and any other issues arising under the safe Harbour, (d) the specific statutory body that has jurisdiction to hear any claims against the organisation regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy (and that is listed in the annex to the Principles), (e) name of any privacy programs in which the organisation is a member, (f) method of verification (e.g. in-house, third party) (1), and (g) the independent recourse mechanism that is available to investigate unresolved complaints.

22 In particular, the Commission services consider that the following changes are necessary: First, an analysis of the organisations that self-certified to the Principles shows that organisations do not always provide a hyperlink to their privacy policy or the one provided does not work. This means that de facto such organisations fail to effectively state where the privacy policy is available, as required under FAQ 6. While the DoC seems to make genuine efforts to review organisations' submissions to certify to the Principles before putting their names in the publicly available Safe Harbour List, the Commission believes that the DoC should apply more stringent controls when checking organisations' compliance with FAQ 6. Second, an important number of organisations that self-certified to the Principles declared to import personal information as data processors. The Safe Harbour decision does not impose any obligation upon organisations to state whether they act as data controller or as data processor. Similar obligation does not exist for the DoC either. However, taking into account that the legal obligations for data processors are different from those of data controllers, it is desirable for the certification form to distinguish between both categories. Third, we note that the DoC's web site lacks a publicly available search function which would allow identifying a given company without having to scroll through the whole list of organisations that certified to the Principles. In order to enhance transparency of information regarding organisations that subscribe to the Principles and to facilitate the use of the

Contrary to the requirement contained in FAQ 9, the Commission services note that the on-line form to self-certify to the Principles available on the DoC's web site does not provide a box for organisations to state their commitment to comply with the advice given by the EU panel in the event of a dispute.[23] Furthermore, if organisations made such a statement in their paper based self-certification letters, the statement is currently not reproduced on the DoC web site as a part of the DoC obligation to make the letters publicly available. As noted in section II, the lack of publication of such a statement may mean that the statement is not enforceable vis-à-vis the organization.

For the moment, the EU panel has never been called to hear complaints from data subjects and therefore the FTC's inability to enforce compliance with the advice of the EU panel has not been tested. However, for the future, the Commission services will request the US DoC to change its website to include a mandatory box for organisations to state their commitment to comply with the advice of the EU panel. Moreover, the Commission services will ask the DoC not to list as Safe Harbour members companies that opt for the EU panel but fail to commit to comply with the advice of the EU panel on their self-certification letters.

IV. ASSESSMENT OF VARIOUS ORGANISATIONS' COMPLIANCE WITH SAFE HARBOUR REQUIREMENTS

1. Federal Trade Commission

The Federal Trade Commission is the main competent body to enforce the Safe Harbour Principles[24]. Pursuant to Article 5 of the FTC Act, the FTC's jurisdiction extends to unfair or deceptive acts or practices affecting commerce.

The Commission services consider that there are instances where the FTC's intervention is necessary to address some of the shortcomings identified in this report. Among other things, the FTC could undertake *sua sponte* investigations where questions exist regarding Safe Harbour compliance, and the FTC could be more proactive in encouraging data subjects to protect their rights and to seek FTC intervention. In addition, the FTC could inform all Safe Harbour members about what it regards as necessary to meet the requirement to have a "publicly available privacy policy" and state its intention to initiate actions against those who have not met this requirement by a certain date.

Another area of concern for the Commission services is the enforcement of the Safe Harbour Principles regarding human resources data. Because the FTC's enforcement competence is limited to deceptive practices "affecting commerce", the extent to which the FTC has

---

DoC's web site, it would be desirable if such a function was incorporated into the DoC web site. Fourth, on the issue of the certification status, as even if a company withdraws its Safe Harbour adherence, it continues to be bound by the terms of the privacy policy under which it imported data, the Commission believes that it would be appropriate to add to the DoC web site a list of companies that have withdrawn their adherence.

23 FAQ 9, section 4, second paragraph says: "A U.S. organisation participating in the Safe Harbour that uses EU human resources data transferred from the European Union in the context of the employment relationship and that wishes such transfers to be covered by the Safe Harbour must therefore commit to cooperate in investigations by and to comply with the advice of competent EU authorities in such cases".

24 Pursuant to the Safe Harbour decision, the other competent body to enforce the Safe Harbour Principles is the Department of Transportation on the basis of its authority under Title 49 United States Code Section 41712.

competence to enforce the Safe Harbour Principles regarding human resources data is not clear. The question is particularly relevant if one takes into consideration that up to 30 percent of the companies that subscribe to the Safe Harbour Principles do so to import human resources data. Given the relevant number of companies that import human resources data and lack of confirmation by courts, obtaining clear guidance from the FTC regarding its competence to enforce the Principles regarding such data is crucial. Hence, the Commission will request the FTC to clarify this issue. Alternatively, a declaratory judgment by a federal court or statutory modifications from Congress could also possibly clarify this question.

2. Organisations providing alternative recourse mechanisms

According to the enforcement Principle, organisations receiving personal data from the EU must commit to apply mechanisms that ensure compliance with the Principles. Pursuant to the enforcement Principle as interpreted by FAQ 11, FAQ 5 and FAQ 6, this requirement can be met by adhering to independent recourse mechanisms that have publicly stated their competence for hearing individual complaints for failure to abide by the Principles.Alternatively, it can be done through the organisation's commitment to cooperate with the EU panel. Other methods are also possible. In November 2003, 73 percent of the organisations had certified their willingness to co-operate with the EU panel. The others selected alternative recourse mechanisms. Let us look into the requirements for alternative recourse mechanisms.

The enforcement Principle and FAQ 11 impose certain rules upon alternative recourse mechanisms which have publicly declared themselves as competent to hear complaints concerning alleged violations of the Safe Harbour Principles, including: (i) they should be readily available, independent and affordable; (ii) they should provide individuals with information about how the dispute resolution procedure works when they file a complaint, including the alternative recourse mechanisms' privacy practices; (iii) they must undertake to remedy problems arising out of organisations' failure to abide by the Principles and (iv) they must foresee rigorous sanctions that would deter companies from further violation of the Principles. These sanctions must include the publicity for findings of non-compliance and the requirement to delete data in certain circumstances. Other potential sanctions may include removal of a seal and compensation to the individual for losses.

A number of alternative recourse mechanisms provide their services regarding the Safe Harbour. Among others these include the following: TRUSTe, Direct Marketing Association Safe Harbour Program, BBBOnline, American Arbitration Association. Up until now, ADRs report that the number of complaints regarding Safe Harbour have been insignificant, which means that there is little experience on which to determine if ADRs carry out their roles properly. It is possible, however, to analyse whether alternative recourse mechanisms comply with the requirements set forth by the enforcement Principle and FAQ 11, and in this regard, the Commission services have detected some failures. As far as requirement (ii) is concerned, the Commission services note some alternative recourse mechanisms lack transparency insofar as they operate without properly informing individuals as to how the dispute resolution procedure works to file a complaint for alleged failure to abide by the Principles. The Commission services have observed that a fair number of the alternative recourse mechanisms that were reviewed do not comply with requirement (iii), i.e., they do not seem to foresee ways to remedy situations of failure to abide by the Principles. Finally, as far as sanctions are concerned, the Commission services observe a trend among the alternative recourse mechanisms analysed of not including the mandatory sanction consisting in the publication of findings of non compliance.

Alternative recourse mechanisms are vital in order to ensure that individual complaints and disputes are investigated and resolved by reference to the Safe Harbour Principles. Providing data subjects with effective means of enforcing their rights is a key element of the Safe Harbour decision and the failure of Safe Harbour members to provide such means undermines an essential element of the system. The Commission considers that it is critical for this issue be remedied rapidly.

3. Panel of EU data protection authorities

As described above, organisations that certify to the Safe Harbour Principles must choose to comply with independent recourse mechanisms or to cooperate with the EU panel. The option of the EU panel is mandatory when human resources data are transferred from the EU to an organisation that has self-certified to the Principles. If the organisation commits itself to cooperate with the EU panel, it must also commit itself to comply with any advice given by the EU panel where these take the view that the organisation needs to take specific action to comply with the Principles[25]. Failure to comply with the panel's advice may constitute a deception or misrepresentation under the FTC Act.

The EU panel has a website: (http://forum.europa.eu.int/Public/irc/secureida/safeHarbour/home), which contains a standard complaint form, the list of data protection authorities operating in the panel, etc.

Neither organisations nor individuals have ever referred complaints to the EU panel which has therefore never delivered any advice. This may be due to the lack of general information at European and US levels about the existence of the EU panel. The Commission services will take various initiatives to raise awareness of the existence of the EU panel. In particular, the Commission services will post a link to the panel on its web site. Furthermore, the Commission services will discuss the issue with national data protection authorities to encourage them to post links to the EU panel. The Commission services will also encourage EU data protection authorities to place national language versions of the complaint form on their web site.

V. RISK OF DISCRIMINATORY EFFECTS OF THE DECISION

According to Article 4 of the Safe Harbour decision, the Commission must report on whether evidence exists that the decision is being implemented in a discriminatory way**.** The Commission does not perceive any sign of discrimination, for example discrimination of one company or economic sector versus others, in the effective implementation of the Safe Harbour decision. In addition, the Commission considers that, since the approval of the Safe Harbour decision, any adequacy decision has been adopted on the basis of third countries' legislation or agreements imposing fewer obligations on data controllers than the Safe Harbour decision, hence discriminating against the United States.

The Commission services confirm this has not been the case. In particular, the Commission confirms that it has not discriminated against the United States or any other third country by

25 FAQ 5 and FAQ 9 set forth the scope of the cooperation between organisations and EU panel which in a nutshell is foreseen as follows: First, the EU authorities will work through a panel which will react in response to referrals from individuals or from organisations. After hearing both parties, the panel will provide advice which will seek to ensure that the principles are being correctly applied and which may include potential remedies.

adopting an arrangement with other countries setting forth less stringent requirements than the Safe Harbour decision. The Commission services have reviewed third countries' legislation for the purposes of adopting an adequacy decision and it has always subjected such third country legislation, as the Safe Harbour, to the privacy standards set forth in Working document 12 adopted by Working Party 29 entitled "Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection Directive"[26]. In applying such standards, various adequacy decisions have been granted whereas some proposals for adequacy decisions have been denied for not meeting the standards.

VI. CONCLUSIONS

On the basis of the information collected either directly by the Commission services or through the contractor's study, the Commission has reached the conclusions described below regarding the implementation of the Safe Harbour decision. It should be noted that the findings of this report are in line with those of the Commission Staff Working Paper adopted in 2002.

Firstly, the Commission is pleased to see that the Safe Harbour has been embraced by more than 400 US organizations. This represents a constant growth in membership. The Commission finds this encouraging insofar as otherwise it is uncertain whether the transfer of data made to these organisations would have been made subject to the same level of protection. At the same time, the Commission considers that it would be positive if membership were to increase further. In future reports, the Commission may consider analysing the market share of the organisations that subscribe to the Safe Harbour or at least the market share of a specific sector to obtain an accurate indication of the Safe Harbour level of membership, at least in a specific sector.

Secondly, in assessing organisations' compliance with the Principles, the Commission services are concerned about the number of self-certified organizations that have not published a privacy policy or that have published a policy that is not compliant with the Principles. The Commission services consider that this creates a problem not only because under the Safe Harbour having a publicly available privacy policy is mandatory, but also, because the absence of a privacy policy or of one fully consistent with the Principles means that the FTC has no jurisdiction to enforce the missing Principles upon the organizations that failed to publish them. The Commission services will work together with the US authorities to reverse this trend. To this end, the Commission has made several suggestions to the DoC including asking it to be more active in scrutinizing US organisations that self-certify to the Principles in order to avoid listing on the Safe Harbour List companies lacking a publicly available privacy policy. The Commission also considers this to be one of the instances where it is essential for the FTC to be more proactive in monitoring organisations' compliance with the Principles and launching investigations where questions exist regarding Safe Harbour compliance.

Thirdly, regarding the functioning of the DoC as the body competent for ensuring self-certification, in general, the Commission finds that it is carrying out its role in accordance with the Safe Harbour requirements. However, the Commission suggests that the DoC should implement various changes to its web site which would, *inter alia*, enhance its transparency. In particular, the DoC web site should provide a box for organisations to state their

26 Adopted on July 24, 1998. DG XV D/5025/98.

commitment to comply with the advice given by the EU panel in the event of a dispute without which the FTC would be unable to enforce compliance with the advice of the EU panel.

Fourthly, regarding alternative recourse mechanisms and the EU panel as enforcement bodies, while the Commission services are pleased that such bodies exist and are available for hearing individuals' complaints, the Commission services note some problems. In particular, some alternative recourse mechanisms still fail to comply with applicable Safe Harbour requirements, including the obligation to provide for sanctions such as the publication of findings of non compliance. The Commission services consider that this issue, which is key for the good functioning of the Safe Harbour system, should be resolved rapidly.

Finally, the Commission services consider that given that up to 30 percent of the companies that subscribe to the Safe Harbour Principles do so to import human resources data clear guidance as to whether the FTC is competent to enforce the Principles in this area is needed.

The Commission services are fully committed to continue monitoring the implementation of the Safe Harbour decision in order to ensure that the actual operation of the Safe Harbour results in adequate protection of the privacy rights of individuals.