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[1], 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[2] 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[3].

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[4]. 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.

---

[1] 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

[2] 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.

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

[4] 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 [5]

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

[5] 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[6]

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,

[6] 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

Done at Brussels, 7 June 1999

For the Working Party

The Chairman

P.J. HUSTINX