

International data transfers between the United States and the European Union: are the procedural provisions of the Safe Harbor solution adequate?

Alexander Zinser, Lausanne, Switzerland

Data transfers out of the European Union are only admissible if the third country ensures an adequate level of protection. With regard to the United States, organizations may adhere to so-called Safe Harbor principles whereby an adequate level of protection is admitted. This article reviews the relevant procedural provisions on granting the Safe Harbor status. It concludes that the current system does not really safeguard compliance with the Safe Harbor principles.

A. Introduction

The European Union has enacted the Directive 95/46/EC which relates to the processing of personal data and on the free movement of data (“Directive”).¹ The Directive makes sure that personal data can be transferred without restrictions within the European Union: Member States are prohibited from restricting the freedom of data transfers by arguing that another Member State will not have an adequate level of data protection.² However, the Directive also regulates the transfer of data out of the European Union: According to Article 25 of the Directive, such a transfer may take place only if the third country in question ensures an adequate level of protection. With regard to data transfers from the European Union to the United States, the United States would need to ensure an adequate level of protection in order to be in compliance with European data protection laws.

In order to fulfil the adequacy requirement, the United States and the European Commission worked on the so-called Safe Harbor solution for United States companies, which voluntarily choose to adhere to certain data protection principles. The negotiations were finalised by the European Commission’s Decision on Safe Harbor whereby:

For the purposes of Article 25(2) of Directive 95/46/EC, for all the activities falling within the scope of that Directive, the Safe Harbor Privacy Principles ... implemented in accordance with the guidance provided by the frequently asked questions ... are considered to ensure an adequate level of protection for personal data

*transferred from the Community to organizations established in the United States.*³

The concept is that the Safe Harbor Principles issued by the United States Department of Commerce on July 21, 2000⁴ and the accompanying Frequently Asked Question⁵ set forth the provisions ensuring the adequate level of data protection.

B. Procedure

An organization based in the United States needs to agree to the Safe Harbor Principles. Several avenues are available for meeting the Safe Harbor Principles: a) agreeing to comply with a private sector data protection program incorporating the Safe Harbor Principles in its rules; b) complying with a statutory, regulatory or administrative authority having dispute resolution and complaints procedure powers; c) agreeing to adhere to any data protection authority situated in Europe; d) agreeing to comply with any other private sector self regulatory scheme provided that the scheme is in line with the enforcement principle and provided that any failure of the scheme to self-regulate is actionable under Section 5 of the United States Federal Trade Commission Act.⁶

However, an organization must also publicly declare that it complies with the Safe Harbor Principles. It may benefit from the Safe Harbor arrangement as soon as it self-certifies to the United States Department of Commerce. The certification can also be submitted online.⁷ Such a certification will not last forever: an organization needs to self-certify annually to the United States Department of Commerce that it adheres to the Safe Harbor’s requirements, and it must continue to follow the Safe Harbor requirements. The United States Department of Commerce also highly recommends that the organization sets out in its published privacy policy statement that it adheres to the Safe Harbor Principles. A list of all organizations that register through the website or through a letter⁸ is maintained by the United States Department of Commerce.⁹

An organization based in the United States needs to agree to the Safe Harbor Principles

In connection with the certification for Safe Harbor, at least the following information must be submitted:

- name, mailing address, e-mail address, telephone and fax numbers of the organization;
- a description of the activities of the organization with regard to personal information transmitted from the European Union;
- a description of the organization's privacy policy for such personal information.

This description must include information on:

- the place where the privacy policy is available for viewing by the public;
- the effective date;
- the contact office for the handling of complaints, access and other requests arising under Safe Harbor;
- the specific statutory body that has jurisdiction to hear any claims against the organization with regard to violations of data protection laws;
- the name of any privacy programs in which the organization is a member;
- the method of verification; and
- the independent recourse mechanism that is available to investigate unresolved complaints.¹⁰

C. Verification of compliance with the Safe Harbor Principles

An organization may verify the compliance with the Safe Harbor Principles through self-assessment or outside compliance reviews. The self-assessment approach would be that the organization has to indicate in the verification form that its published data protection policy regarding personal information received from the European Union is accurate, comprehensive, prominently displayed, completely implemented and accessible. Also, an indication is needed that the policy conforms to the Safe Harbor Principles; that individuals are informed of any in-house arrangements for handling complaints; that training procedures for employees are in place. Organizations should hold a copy of the procedure of implementation of the Safe Harbor Principles and make them available upon request by individuals or in the context of an investigation or a complaint about compliance.¹¹

An outside compliance review needs to demonstrate that the data protection policy regarding personal information received from the European Union conforms to the Safe Harbor Principles and that individuals are informed on the

mechanisms through which they may pursue complaints. The review may include auditing, random reviews and use of technology tools as appropriate. A copy of the statement verifying that an outside compliance review has been successful should be available upon request.¹²

D. Persistent failure to comply

When an organization does not persistently comply with the Safe Harbor Principles, it is no longer allowed to take advantage of Safe Harbor status. Persistent failure to comply may arise in the following cases: refusal to comply with a final determination by any self-regulatory body or government body or a claim to comply with the Safe Harbor Principles where such an aforementioned body determines that a frequent failure to comply takes place. The organization is obliged to promptly notify the United States Department of Commerce of such cases. If it fails to do so, it may be actionable under the False Statements Act. The United States Department of Commerce shows a notification of a persistent failure to comply on the list of all self-certified organizations. The notification may be submitted from the relevant organization, from a self-regulatory body or from a government body. However, before such an indication will be shown on the list, the organization that did not comply must be provided with a thirty days' notice and an opportunity to respond. The list maintained by the United States Department of Commerce will show which organization may benefit from Safe Harbor and which organization is not entitled to take advantage from it.¹³

E. Powers of the authorities

The European data protection authorities have the power to suspend data transfers to an organization which has self-certified for Safe Harbor. However, such an action can only be taken if:

- A United States government body or an independent recourse has determined non-compliance with the Safe Harbor Principles;
- There is a substantial likelihood of a risk of grave harm to data subjects and of non-success of relevant enforcement actions.

The national data protection authorities have to inform immediately the European Commission of any suspension. The European Commission is obliged to inform the United States Department of Commerce in case that there is enough evidence

that a body responsible for ensuring compliance with the Principles does not fulfil its role. Furthermore, the European Commission may draft measures aiming at the suspension or reversal the Decision on Safe Harbor.¹⁴ In other words, in practice, the European Commission can reverse the Decision whereby the Safe Harbor arrangement has been granted adequate protection status.¹⁵

F. Criticism and conclusion

The website listing the companies which adhere to the Safe Harbor Principles is very helpful for the review of the legality of the international data transfer in question: looking at the list, companies in the European Union know to which organizations based in the United States they can transfer data without establishing other safeguards. Also, European Union citizens have a clear picture which organization has joined Safe Harbor and, therefore, they know which organization has a proper data protection regime in place.

The system of self-certification does not ensure that all companies which have joined Safe Harbor, fulfil the relevant requirements. Certainly, it is quite easy to fill in the online form. However, in practice, the question must be asked whether the statements submitted are true and reliable. Instead of the system of self-certification, companies should only benefit from Safe Harbor where an independent body has reviewed the data protection regime of the organization intending to join Safe Harbor. An explicit consent of the relevant authority should be needed before the Safe Harbor status will be granted.

The right of the European data protection authorities to suspend data transfers seems to be appropriate. However, such an action can only be taken if a United States government body or an independent resource acting on behalf of such a governmental body has determined non-compliance with the Safe Harbor Principles. Efficient supervisory authorities need to review the relevant situations. In practice, however, such supervisory authorities are only established to a limited extent in the United States. Therefore, it can be said that the suspension right of the European data protection authorities is undermined by the system in the United States to some extent. Apart from that, the European Commission has the power to reverse the Decision.

If the European Commission takes such a decision, at least an interim solution is needed. From a practical point of view, it is logical to draft a provision whereby the European Commission may only reverse the Decision by keeping within certain time limits.

Alexander Zinser Dr. jur; LL.M.; Senior Attorney at Agilent Technologies International Sarl, Morges, Switzerland, a subsidiary of Agilent Technologies Inc, Palo Alto, California. Dr. Alexander Zinser, LL.M.; Avenue de l'Eglantine 14, CH-1006 Lausanne, Switzerland. Tel.: +41 (0) 21 811 3828; Fax: 41 (0) 21 811 3896; e-mail: alexander_zinser@agilent.com

The views expressed in this article are the author's own and do not necessarily reflect those of Agilent Technologies.

FOOTNOTES

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 data; [1995] O.J. L 281/31.

2 David I. Bainbridge, Processing personal data and the Data Protection Directive, 6 *Information & Communications Technology Law*, March 17, 18 (1997).

3 Art. 1 of the Decision regarding the Safe Harbor Principles as an adequate level of protection ("Decision"); [2000] O.J. L 215/7; the document is available from http://europa.eu.int/comm/internal_market/en/dataprot/ad_equacy/index.htm.

4 Available from <http://www.export.gov/safeharbor>; hereinafter referred as "Safe Harbor Principles".

5 Available from <http://www.export.gov/safeharbor>; hereinafter referred as "Frequently Asked Question".

6 Piers Leigh-Pollitt/James Mullock, *The Data Protection Act*, 157 (Third Edition, 2001).

7 The online certification form is available from <http://web.ita.doc.gov/safeharbor/shreq.nsf/safeharbor?openform>.

8 The list is available from <http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list>.

9 See Department of Commerce, Safe Harbor Workbook, available from http://www.export.gov/safeharbor/sh_workbook.html.

10 See Frequently Asked Question 6; available from <http://www.export.gov/safeharbor/FAQ6SelfCertFINAL.htm>.

11 See Frequently Asked Question 7; available from <http://www.export.gov/safeharbor/Faq7veriffINAL.htm>.

12 See Frequently Asked Question 7; available from <http://www.export.gov/safeharbor/Faq7veriffINAL.htm>.

13 See Frequently Asked Question 11; available from <http://www.export.gov/safeharbor/FAQ11FINAL.htm>.

14 Art. 3 of the Decision.

15 Tanguy van Overstraeten/Emmanuel Szafran, Data protection and privacy on the internet: technical considerations and European legal framework, 7 *C.T.L.R.* 56, 64 (2001).

The right of the European data protection authorities to suspend data transfers seems to be appropriate