

Draft Frequently Asked Questions (FAQs)

FAQ 6 - Self-Certification

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

A: Safe harbor benefits are assured from the date on which an organization self-certifies to the Department of Commerce (~~for its designee~~) **nominee its adherence to the principles in accordance with the guidance set forth below.**

To self-certify for the safe harbor, organizations can provide to the Department of Commerce (or its designee) a letter, signed by a corporate officer on behalf of the organization that is joining the safe harbor, that contains at least the following information:

- 1. name of organization, mailing address, email address, telephone and fax numbers;**
- 2. description of the activities of the organization with respect to personal information received from the EU;**
- 3. description of the organization's privacy policy for such personal information, including:**
 - a. where ~~it~~ **the privacy policy** is available for viewing by the public,**
 - b. its effective date of implementation,**
 - c. a contact ~~person~~ **office** for the handling of complaints, access requests, and any other issues arising under the safe harbor,**
 - d. the specific statutory body that has jurisdiction to hear any claims against the organization 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 organization is a member,**

- f. **method of verification (e.g. in-house, third party)*, and**
- g. **the independent recourse mechanism that is available to investigate unresolved complaints.**

Where the organization wishes its safe harbor benefits to cover human resources information transferred from the EU for use in the context of the employment relationship, it may do so where there is a statutory body with jurisdiction to hear claims against the organization arising out of human resources information that is listed in the annex to the Principles. In addition the organization must indicate this in its letter and declare its commitment to cooperate with the EU authority or authorities concerned in conformity with FAQ 9 and FAQ 5 as applicable and that it will comply with the advice given by such authorities.

The Department ~~of Commerce~~ (or its designee) will maintain a list of all organizations that file such letters, thereby assuring the availability of safe harbor benefits, and will update such list on the basis of annual letters and notifications received pursuant to FAQ 11. Such self certification letters should be provided not less than annually. Otherwise the organization will be removed from the list and safe harbor benefits will no longer be assured. 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 relevant published privacy policy statements that they adhere to the safe harbor principles.

The undertaking to adhere to the safe harbor principles is not time-limited in respect of data received during the period in which the organization enjoys the benefits of the safe harbor. Its undertaking means that it will continue to apply the principles to such data for as long as the organization stores, uses or discloses them, even if it subsequently leaves the safe harbor for any reason.

An organization that will cease to exist as a separate legal entity as a result of a merger or a takeover must notify the Department of Commerce (or its designee) of this in advance. The notification should also indicate whether the acquiring entity or the entity resulting from the merger will (1)

continue to be bound by the safe harbor principles by the operation of law governing the takeover or merger or (2) elect to self-certify its adherence to the safe harbor principles or put in place other safeguards, such as a written agreement that will ensure adherence to the safe harbor principles. Where neither (1) nor (2) applies, any data that has been acquired under the safe harbor must be promptly deleted.

An organization does not need to subject all personal information to the safe harbor principles, but it must subject to the safe harbor principles all personal data received from the EU after it joins the safe harbor.

Any misrepresentation 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 government body. Misrepresentations to the Department of Commerce (or its designee) may be actionable under the False Statements Act (18 U.S.C. § 1001).

***See FAQ on verification**