U.S. Department of Commerce Safe Harbor Certification Review Process

Although it is true that the U.S.-EU Safe Harbor Framework and the U.S.-Swiss Safe Harbor Framework operate as a self-certification program, it is also true that the International Trade Administration (ITA) at the U.S. Department of Commerce plays an important oversight role in administering the program. The ITA's Safe Harbor Team reviews every Safe Harbor certification and annual recertification submission that it receives to ensure that these include all of the elements required by the Frameworks (i.e., the Safe Harbor Privacy Principles and the Frequently Asked Questions and answers that clarify and supplement the Principles) in accordance with guidance provided by the ITA. When an organization's Safe Harbor submission falls short, the ITA contacts the organization by e-mail to explain what is lacking and what steps must be taken before the organization's certification or recertification may be finalized.

What does the ITA look for?

Once the ITA receives the online certification or recertification submission and applicable processing fee, the ITA reviews the organization's Safe Harbor submission within 7 business days, focusing on the following elements:

- Did the organization include appropriate contact information, including a U.S. mailing address, as well as the respective phone numbers and e-mail addresses of the organization's principal point of contact (i.e., individual or office responsible for handling complaints, access requests, and any other issue involving the organization under the Safe Harbor Framework(s)) and the organization's corporate officer responsible for its (re)certification?

- Did the organization provide a reasonable description of its activities with regard to the personal data it receives from the EU/EEA and/or Switzerland?

- Did the organization indicate what personal data is covered by its Safe Harbor (re)certification?

    - Note that an organization may elect to cover all or some specified subset of the personal data it receives, but must specify whether it covers manually processed data.

- Did the organization's response as to whether or not the (re)certification covers its own human resources (hereinafter "HR") data (i.e., personal information about the organization's own employees, past or present, collected in the context of the employment relationship) align with the description it provided of its activities with regard to personal data it receives from the EU/EEA and/or Switzerland?

- If the (re)certification covers an organization's customer/client data, did the organization provide the URL for its publicly accessible privacy policy statement or upload a copy of the privacy policy statement to its Safe Harbor submission?

    - Note that it is mandatory that an organization with a public website make its privacy policy statement(s) for customer/client data readily available on its public website (i.e., it is not sufficient to simply upload a document to its Safe Harbor submission). If an organization does not have a public website, then it must upload a copy of the privacy policy statement to its submission.

    - Note as well that a document uploaded to a submission will become publicly accessible if and when the (re)certification is finalized.

- If the (re)certification covers an organization's own HR data, did the organization 1) provide the URL for its publicly accessible HR-relevant privacy policy statement or upload a copy of its HR-relevant privacy policy statement to its Safe Harbor submission; or 2) provide the ITA with a copy of its HR-relevant privacy policy statement for review and explain in its submission how its employees may obtain a copy?
    - Note that while it is recommended that an organization make its HR-relevant privacy policy statement readily available on its public website or as a document uploaded to its Safe Harbor submission, it is mandatory that an organization make its HR-relevant privacy policy statement accessible to affected employees.
- Did each one of the privacy policy statements provided include an affirmative commitment to the U.S.-EU Safe Harbor Framework and/or U.S.-Swiss Safe Harbor Framework?
    - Note that an organization can (re)certify its compliance with one or both of the Safe Harbor Frameworks, but the organization's Safe Harbor submission and privacy policy statement(s) must be consistent on this point.
    - Note as well that each review also includes a determination as to whether the organization is using the U.S.-EU Safe Harbor Framework certification mark, and if so, whether it is doing so in accordance with the instructions set forth by the ITA on the Safe Harbor website.
    - In addition, organizations are strongly encouraged – both in the guidance provided on the Safe Harbor website and in e-mail messages sent during the review process – to include in their privacy policy statement(s) either a hyperlink to the Safe Harbor website and/or the corresponding URL (e.g., http://export.gov/safeharbor/).
- Did the organization indicate which U.S. regulator (i.e., either the U.S. Federal Trade Commission or the U.S. Department of Transportation) has jurisdiction over any claims against the organization and does that designation seem appropriate in the context of the activities described?
- Did the organization indicate how it verifies, at least annually, that its Safe Harbor attestations are accurate (i.e., that the privacy practices have been implemented as represented and in accordance with the Safe Harbor Privacy Principles)?
    - Note that an organization can use either in-house or third party verification.
- Did the organization identify at least one appropriate independent recourse mechanism (i.e., third party dispute resolution provider) that is available to receive and adjudicate unresolved complaints alleging that the organization has violated its Safe Harbor attestations?
    - Note that when it comes to customer/client data an organization may either use a specified private sector provider or cooperate and comply with appropriate (i.e., EU and/or Swiss) data protection authorities; however, when it comes to its own HR data an organization must cooperate and comply with the appropriate (i.e., EU and/or Swiss) data protection authorities. Even if an organization uses a specified private sector provider for its customer/client data, the organization may also voluntarily agree to cooperate and comply with appropriate (i.e., EU and/or Swiss) data protection authorities.
    - Note as well that organizations are strongly encouraged – both in the guidance provided on the Safe Harbor website and in e-mail messages sent during the review process – to include in their privacy policy statement(s) a clear reference to appropriate independent recourse mechanism(s), as well as relevant contact information for said mechanism(s).

- If the organization indicated that the (re)certification covers its own HR data, did it agree to cooperate and comply with the appropriate data protection authorities?

What does the ITA do if all of the aforementioned elements are complete?

- The ITA finalizes the organization's (re)certification:
    - In the case of a new certification, the organization's record is added to the public Safe Harbor List(s) featuring a "Certification Status" designation of "Current" and a "Next Certification" date marking the anniversary of the day when the new certification was finalized. The ITA notifies the organization's listed "Organization Contact" by e-mail that the certification has been finalized.
    - In the case of a recertification, the "Certification Status" is designated as "Current" and the "Next Certification" date is updated in the organization's record on the public Safe Harbor List(s). The ITA does not ordinarily notify the organization's listed "Organization Contact" that the recertification has been finalized, as an organization's record on the public Safe Harbor List(s) serves as notice of the organization's "Certification Status".

What does the ITA do if any of the aforementioned elements is missing or incomplete?

- The ITA contacts the listed "Organization Contact" by e-mail and explains which elements are lacking or require clarification and describes how this may be rectified
- Once the organization rectifies the issue(s) identified, the ITA finalizes the organization's (re)certification
    - Note that for a new certification the certification will last one year from the day it is finalized, whereas for a recertification the certification will only last until its next recertification falls due, which ordinarily is the anniversary of the day its original certification was finalized.
- If the organization fails to rectify the issues identified, the ITA does not finalize the organization's (re)certification:
    - In the case of a new certification, the organization never appears on the public Safe Harbor List(s).
    - In the case of a recertification, the "Certification Status" is designated as "Not Current" in the organization's record on the public Safe Harbor List(s). The ITA notifies the organization's "Organization Contact" by e-mail that its Safe Harbor certification has lapsed.

For any questions regarding the review process, please feel free to contact the ITA's Safe Harbor Team at Safe.Harbor@trade.gov