Federal Trade Commission Enforcement of the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks

Tags: Privacy and Security | U.S.-EU Safe Harbor Framework

Update on the U.S.-EU Safe Harbor Framework

On October 6, 2015, the European Court of Justice issued a judgment declaring invalid the European Commission's July 26, 2000 decision on the legal adequacy of the U.S.-EU Safe Harbor Framework. On July 12, 2016, the European Commission issued an adequacy decision on the EU-U.S. Privacy Shield Framework. This new Framework, which replaces the Safe Harbor program, provides a legal mechanism for companies to transfer personal data from the EU to the United States. The FTC will enforce the Privacy Shield Framework. We continue to expect companies to comply with their ongoing obligations with respect to data previously transferred under the Safe Harbor Framework. More information on the new framework is on the FTC's Privacy Shield Framework page. Updated on July 25th, 2016.

In 2000, the European Commission, together with the U.S. government, created the U.S. – EU Safe Harbor Framework. On December 10, 2008, the Department of Commerce finalized negotiations with the Government of Switzerland to launch a U.S.-Swiss Safe Harbor Framework. The Swiss Framework went into force in February 2009 and parallels the U.S.-EU Framework. The U.S.-Swiss Framework allows U.S. companies to meet the requirements of the Swiss Federal Act on Data Protection.

To join the U.S.-EU Safe Harbor, a company must self-certify to the Commerce Department that it complies with seven principles and related requirements. The FTC enforces the promises that companies make when they certify that that they participate in the Safe Harbor Framework.

The seven Principles in the U.S.-EU Safe Harbor Framework are:

1. Notice

Organizations must notify individuals about the purposes for which they collect and use information about them. They must provide information about how individuals can contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information and the choices and means the organization offers for limiting its use and disclosure.

2. Choice

Organizations must give individuals the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or later authorized by the individual. For sensitive information, affirmative or explicit (opt in) choice must be given if the

information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorized subsequently by the individual.

3. Onward Transfer (Transfer to Third Parties)

To disclose information to a third party, organizations must apply the notice and choice principles. Where an organization wishes to transfer information to a third party that is acting as an agent, it may do so if it makes sure that the third party subscribes to the Safe Harbor Privacy Principles or is subject to the Directive or another adequacy finding. As an alternative, the organization can enter into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles.

4. Access

Individuals must have access to personal information about themselves that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

5. Security

Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.

6. Data Integrity

Personal information must be relevant for the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

7. Enforcement

To ensure compliance with the Safe Harbor principles, there must be: (a) readily available and affordable independent

To ensure compliance with the Safe Harbor principles, there must be: (a) readily available and affordable independent recourse mechanisms so that each individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) procedures for verifying that the commitments companies make to adhere to the Safe Harbor principles have been implemented; and (c) obligations to remedy problems arising out of a failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization. Organizations that fail to provide annual self-certification letters will no longer appear in the list of participants.

December 2012