FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Information for EU Residents Regarding the U.S. – EU Safe Harbor Program

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

annexes_eu-us_privacy_shield_en1.pdf (1.45 MB)

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.

Under European Union (EU) law, personal data – including your name, address or social networking profile – can only be gathered legally under specific conditions, for a legitimate purpose. Companies in the EU that collect and manage your personal information must protect it from misuse and must respect certain rights guaranteed by EU law.

The EU's Data Protection Directive also has specific rules for the transfer of personal data outside of the EU to maintain the protection of your data when it is exported abroad.

Under EU law, personal data generally may be transferred only to a non-EU country that provides an adequate level of privacy protection. The European Commission, together with the U.S. government, created the U.S. – EU Safe Harbor Framework. On July 26, 2000, the European Commission determined that companies participating in the Framework provide an "adequate level of protection" for EU data.

The protections under the Safe Harbor Framework fall under seven Principles:

- Notice: A Safe Harbor company must inform you about its information practices, including the purposes for which it collects and uses personal data, the company contact information, the types of third parties it transfers the data to, and what choices you have for limiting uses and disclosures.
- Choice: A Safe Harbor company must give you the opportunity to choose how your personal

Notice: [illegible] information is used and disclosed to third parties.

- Onward Transfer: A Safe Harbor company may disclose data to a third party only under certain conditions, and it must ensure that the data remains protected at least at the same level as is required under Safe Harbor Principles or otherwise in accordance with EU law.

- Security: A Safe Harbor company must take reasonable steps to prevent loss, misuse or unauthorized disclosures.
- Data Integrity: A Safe Harbor company must only collect data that is relevant for purposes for which it is to be used and should take reasonable steps to keep it current.

- Access: As a general rule, a Safe Harbor company must provide you access to your data and an opportunity for you to correct or amend inaccurate data.

- Enforcement: A Safe Harbor company must provide you with a mechanism to resolve your dispute over whether it is following the Principles.

To join the Safe Harbor, a company must be subject to the jurisdiction of the Federal Trade Commission (FTC) or the Department of Transportation, and it must self-certify to the U.S. Department of Commerce that it complies with the Safe Harbor Privacy Principles. The Department of Commerce makes information about the Safe Harbor program available on its website. It includes an overview of the program as well as frequently asked questions.

The Department of Commerce also maintains an authoritative list of companies that are current participants in the Safe Harbor program. The FTC has sued companies that claimed in their privacy policies that they were Safe Harbor participants, but were not. The FTC has also sued companies that improperly used the Safe Harbor certification mark, as well as companies that did not comply with the Safe Harbor principles. If you have a question about whether a particular company is a current participant in the Safe Harbor program, you should check the Department of Commerce's list.

You should also check a company's privacy policy to see what claims and promises they make about privacy. Safe Harbor companies that have public websites and use personal data other than their own employees' data are required under the program to make their privacy policies available on their sites. A Safe Harbor company's privacy policy should have details on that company's compliance with Safe Harbor and may describe how it implements the Principles.

February 2015