The U.S. Department of Commerce Safe Harbor used to be a simple $200 investment. All an organization needed was to complete their voluntary online self-assessment form and pay the annual fee. For years, this was done with very little change and no direct enforcement. The process was rarely featured in the news, and companies didn’t rank it high on their compliance checklist.

Recently, however, regulators have started to perform frequent and in-depth audits and taking action against violations. This auditing process has shown that many organizations were not, in fact, in full compliance as they had believed or they did not re-certify after the initial year – even though claiming they did on their website. What had been a $200 permit suddenly started resulting in Federal Trade Commission (FTC) consent decrees. Just last year, twelve U.S. businesses, which included BitTorrent, Inc., Apperian and Reynolds Consumer Products agreed to settle charges with the FTC that each had falsely claimed they were abiding by the U.S.-EU Safe Harbor framework and deceptively claimed they held current certifications. Let us understand how the EU Safe Harbor works and how to help ensure compliance with the laws. Please note there is a Swiss Safe Harbor framework, which is very similar to the EU Safe Harbor, but this report focuses on the EU Safe Harbor.

Solving the Privacy Problem with an Agreement

The basis of the EU Safe Harbor directive comes from the desire to ensure data privacy. The United States and the European Union are both strong proponents of protecting personal data from unauthorized use or transfer, but each region goes about it in a different manner. Pursuing a solution to this problem, the EU entered into an agreement with the U.S. Department of Commerce to develop a set of principles that, when followed by organizations, would provide consumers a level of understanding and expectation about the collection and handling of their personal data. The premise of the EU Safe Harbor is to provide data privacy principles and for the organizations to self-assess and -certify that they’re following them. However, although many organizations have well understood their obligations and compliance responsibilities, others have taken this self-certification approach a lot more casually and fallen out of compliance. Like any other serious program, companies need to utilize governance to ensure the EU Safe Harbor compliance program is managed and accurately represents what its constituents expect.

Can Any U.S. Organization Self-Certify Under the EU Safe Harbor Framework?
The short answer is no. Most U.S. organizations can, but not all. Only those organizations that are subject to the FTC’s jurisdiction can apply for the Safe Harbor certification. This provision excludes organizations in industries that are regulated by other federal agencies such as banking, credit unions and telecommunication to name a few.

Details of Safe Harbor Regulations

In the United States, the Data Protection Act of 1998 requires those who control and process data (also known as data controllers) to register with the Information Commissioners Office (ICO). Institutions such as airline carriers or those subject to the Department of Transportation will need to be Safe Harbor compliant. Organizations such as financial institutions, non-profits and labor associations do not need to register, however, and are regulated by different processes.

Common benefits of this compromise include:

- All European states will be bound by the European Commission’s finding of ‘adequacy’.
- Participating organizations must meet the standards for providing protection considered ‘adequate’.
- Member requirements for prior approval of data transfers either will be waived or approval will be automatically granted.
- Claims brought by EU citizens against U.S. organizations will be heard unless deemed a listed exception to the rules.
- Compliance requirements are designed to benefit small and medium organizations by being streamlined and cost-effective.

Making Compliance Simple

The first step in achieving compliance of the EU Safe Harbor certification is to have a program in place to manage the scope of its requirements. Make it an ongoing exercise to check for compliance either with internal resources or outsourcers.

Compliance checking is based around the seven privacy principles found in the framework. These items include:

Notice - If personal data is being collected, an organization must give those involved individuals proper and reasonable notice. This principle, as well as choice, only applies to the data controller (as opposed to the data processor) as they are the ones collecting data directly from the consumer.

Choice - The data collection process must include an option to opt out. This option must also entail any data shared with third-party services.

Onward Transfer - Data transfers to third parties may only be made if the data is going to organizations that comply with the approved data protection principles.

Security - Data that is collected must be protected with the best and reasonable efforts available.

Data Integrity - Data should only be collected if it is relevant to the reasons it was initially gathered.

Access - The party from which this data was gathered must be able to access their information. This access must include the ability to correct or delete items for accuracy.
**Enforcement** - The above detailed principles must be correctly enforced by the organizations involved, and the ability to enforce these principles must be detailed as needed.

Opting to seek the EU Safe Harbor certification is a business decision. It offers the benefit of open transfer of data between countries with a level of assurance expected by countries and consumers. However, organizations that choose to take this route should develop an ongoing process for demonstrating compliance before it is too late and in the eyes of regulators. With all of the new focus on compliance, it isn't worth taking a chance by blindly checking boxes. For more information for organizations who are unsure of whether or not they should be involved in Safe Harbor regulations, check with the Department of Transportation.