

What is the US Safe Harbor Program?

The European Union's Directive on Data Protection prohibits the transfer of personal data to US companies which do not meet the Commission's standards for privacy protection. To address this issue, the US Department of Commerce established a "safe harbor" framework which was approved by the EU in 2000. US companies that comply are deemed by the EU to have adequate data protection practices, and thus are eligible to receive data from European countries.

Who is affected?

The safe harbor program is a voluntary program for US companies who may receive data from European countries.

What does the Safe Harbor Program have to do with information management?

Companies who participate in the safe harbor program must demonstrate their compliance with seven safe harbor principles concerning information management. One of these principles involves information security. For example, organizations must take reasonable measures to protect personal information from loss, misuse, unauthorized access, disclosure, alteration and destruction.

What do companies have to do to comply with the Safe Harbor Program?

To qualify for the safe harbor program, a company may either join a self-regulatory privacy program that adheres to the safe harbor requirements or develop its own self-regulatory privacy policy that conforms to the safe harbor program. Companies must provide an annual self-certification to the U.S. Department of Commerce, which maintains a public list of all self-certified companies.

Penalties for Non-Compliance?

Participants must have a dispute resolution system, a compliance verification program, and remedy requirements in place. Dispute resolution bodies must have the ability to suspend participants from their privacy program (and thus from the safe harbor program) and to issue injunctive orders.

Further, a company's failure to comply with its self-imposed regulations is actionable under federal or state law prohibiting unfair or deceptive acts. Depending on the industry, the Federal Trade Commission, the Department of Transportation and/or other, similar government agencies may enforce the safe harbor principles against US organizations that are subject to their jurisdiction. For example, the FTC has the power to impose civil penalties of up to \$12,000 per day for violations.

Perhaps most importantly, of course, a company that persistently fails to comply with the safe harbor requirements will be prohibited from receiving personal data from EU countries, which may significantly impact that company's business.

How can we help?

One of the safe harbor principles is information security: participants must keep information secure from unauthorized disclosure and access. When designing information management programs for the safe harbor program, US companies should consider how they store and destroy their customers' information. Securit offers safe document storage and management, and secure on site document destruction. We're committed to limiting the risk of an unauthorized person gaining access to sensitive personal information. For peace of mind, contact Securit today at 1 800 697-4733.

For more information:

U.S. Department of Commerce - <http://www.export.gov/safeharbor/>

This document does not constitute a legal opinion or legal advice. Do not rely on any of the information in this document without first obtaining legal advice.

© Copyright 2006