



## U.S.-EU Safe Harbor Overview

The European Commission's Directive on Data Protection went into effect in October 1998, and would prohibit the transfer of personal data to non-European Union countries that do not meet the European Union (EU) "adequacy" standard for privacy protection. While the United States and the EU share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the EU. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation. The EU, however, relies on comprehensive legislation that requires, among other things, the creation of independent government data protection agencies, registration of databases with those agencies, and in some instances prior approval before personal data processing may begin. As a result of these different privacy approaches, the Directive could have significantly hampered the ability of U.S. organizations to engage in a range of trans-Atlantic transactions.

In order to bridge these differences in approach and provide a streamlined means for U.S. organizations to comply with the Directive, the U.S. Department of Commerce in consultation with the European Commission developed a "safe harbor" framework. The U.S.-EU Safe Harbor Framework, which was approved by the EU in 2000, is an important way for U.S. organizations to avoid experiencing interruptions in their business dealings with the EU or facing prosecution by EU member state authorities under EU member state privacy laws. Self-certifying to the U.S.-EU Safe Harbor Framework will ensure that EU organizations know that your organization provides "adequate" privacy protection, as defined by the Directive.

## U.S.-EU SAFE HARBOR BENEFITS

The U.S.-EU Safe Harbor program provides a number of important benefits to U.S. and EU firms. Benefits for participating U.S. organizations include:

- All 27 Member States of the European Union will be bound by the European Commission's finding of adequacy
- Organizations participating in the U.S.-EU Safe Harbor program will be deemed adequate and data flows to those organizations will continue;
- Member State requirements for prior approval of data transfers either will be waived or approval will be automatically granted; and
- Claims brought by EU citizens against U.S. organizations will be heard in the U.S. subject to limited exceptions.

The U.S.-EU Safe Harbor Framework offers a simpler and cheaper means of complying with the adequacy requirements of EU law, which should particularly benefit small and medium enterprises.

An EU organization can ensure that it is sending information to a U.S. organization participating in the U.S.-EU Safe Harbor program by viewing the public list of Safe Harbor organizations posted on this website. This list contains the names of all U.S. organizations that have self-certified to the U.S.-EU Safe Harbor Framework. This list will be regularly updated, so that it is clear which organizations are assured of Safe Harbor benefits.

## HOW DOES AN ORGANIZATION JOIN?

The decision by U.S. organizations to enter the U.S.-EU Safe Harbor program is entirely voluntary. Organizations that decide to participate in the U.S.-EU Safe Harbor program must comply with the U.S.-EU Safe Harbor Framework's requirements and publicly declare that they do so. To be assured of Safe Harbor benefits, an organization must self-certify annually to the Department of Commerce in writing that it agrees to adhere to the U.S.-EU Safe Harbor Framework's requirements, which includes elements such as notice, choice, access, and enforcement. It must also state in its published privacy policy statement that it adheres to the Safe Harbor Privacy Principles.

To qualify for the U.S.-EU Safe Harbor program, an organization can (1) join a self-regulatory privacy program that adheres to the U.S.-EU Safe Harbor Framework's requirements; or (2) develop its own self-regulatory privacy policy that conforms to the U.S.-EU Safe Harbor Framework.

## WHAT DO THE SAFE HARBOR PRIVACY PRINCIPLES REQUIRE?

Organizations must comply with the seven Safe Harbor Privacy Principles, which require the following:

### 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.

### 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 subsequently 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.

### Onward Transfer (Transfers 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.

### Access

Individuals must have access to personal information about them 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.

### Security

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

### 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.

### Enforcement

In order 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 and safe harbor benefits will no longer be assured.

To provide further guidance, the Department of Commerce has issued a set of frequently asked questions and answers (FAQs) that clarify and supplement the Safe Harbor Privacy Principles.

## HOW AND WHERE WILL THE U.S.-EU SAFE HARBOR BE ENFORCED?

In general, enforcement of the U.S.-EU Safe Harbor will take place in the United States in accordance with U.S. law and will be carried out primarily by the private sector. Private sector self-regulation and enforcement will be backed up as needed by government enforcement of the federal and state unfair and deceptive statutes. The effect of these statutes is to give an organization's U.S.-EU Safe Harbor commitments the force of law vis a vis that organization.

#### **Private Sector Enforcement**

As part of their U.S.-EU Safe Harbor program obligations, organizations are required to have in place a dispute resolution system that will investigate and resolve individual complaints and disputes and procedures for verifying compliance. They are also required to remedy problems arising out of a failure to comply with the principles. Sanctions that dispute resolution bodies can apply must be severe enough to ensure compliance by the organization; they must include publicity for findings of non-compliance and deletion of data in certain circumstances. They may also include suspension from membership in a privacy program (and thus effectively suspension from the U.S.-EU Safe harbor program) and injunctive orders.

The dispute resolution, verification, and remedy requirements can be satisfied in different ways. An organization could meet the requirements by complying with a private sector developed privacy seal program that incorporates and satisfies the Safe Harbor Privacy Principles. If the seal program, however, only provides for dispute resolution and remedies but not verification, then the organization would have to satisfy the verification requirement in an alternate way. An organization could also meet the requirements by complying with government supervisory authorities or by committing to cooperate with the EU data protection authorities.

#### **Government Enforcement**

Depending on the industry sector, the Federal Trade Commission, comparable U.S. government agencies, and/or the states may provide overarching government enforcement of the Safe Harbor Privacy Principles. Where an organization relies in whole or in part on self-regulation in complying with the Safe Harbor Privacy Principles, its failure to comply with such self-regulation must be actionable under federal or state law prohibiting unfair and deceptive acts or it is not eligible to join the safe harbor. At present, U.S. organizations that are subject to the jurisdiction of either the Federal Trade Commission or the Department of Transportation with respect to air carriers and ticket agents may participate in the U.S.-EU Safe Harbor program. The Federal Trade Commission and the Department of Transportation have both stated in letters to the European Commission that they will take enforcement action against organizations that state that they are in compliance with the U.S.-EU Safe Harbor Framework, but then fail to live up to their statements.

Under the Federal Trade Commission Act, for example, an organization's failure to abide by commitments to implement the Safe Harbor Privacy Principles might be considered deceptive and actionable by the Federal Trade Commission. This is the case even where an organization adhering to the Safe Harbor Privacy Principles relies entirely on self-regulation to provide the enforcement required by the Safe Harbor enforcement principle. The FTC has the power to rectify such misrepresentations by seeking administrative orders and civil penalties of up to \$12,000 per day for violations.

**Failure to Comply with the U.S.-EU Safe Harbor Framework Requirements:** If an organization persistently fails to comply with the U.S.-EU Safe Harbor Framework requirements, it is no longer entitled to benefit from the U.S.-EU Safe Harbor. Persistent failure to comply arises where an organization refuses to comply with a final determination by any self-regulatory or government body or where such a body determines that an organization frequently fails to comply with the requirements to the point where its claim to comply is no longer credible. In these cases, the organization must promptly notify the Department of Commerce of such facts. Failure to do so may be actionable under the False Statements Act (18 U.S.C. § 1001).

The Department of Commerce will indicate on the public list it maintains of organizations self-certifying adherence to the U.S.-EU Safe harbor Framework requirements any notification it receives of persistent failure to comply and will make clear which organizations are assured and which organizations are no longer assured of U.S.-EU Safe Harbor benefits.

An organization applying to participate in a self-regulatory body for the purposes of re-qualifying for the U.S.-EU Safe Harbor program must provide that body with full information about its prior participation in the U.S.-EU Safe Harbor program.