

New England In-House

Seeking Safe Harbor From European Union Privacy Laws



Maria Recalde
nationals.

By Maria Recalde

Many U.S. organizations doing business in the European Union (EU) via the Internet are still unaware of the EU's comprehensive privacy legislation that affects transatlantic online transactions, even though the measure went into effect nearly five years ago.

The European Commission Directive on Data Protection (EU Directive) prohibits online transfers of personally identifiable information to non-EU countries unless an "adequate" level of privacy protection is observed. The EU Directive applies to every organization in the U.S. collecting or receiving personal data about EU nationals online.

Because the patchwork of U.S. privacy laws do not conform to the EU's privacy standards, they are not deemed an "adequate" level of protection. As a result, the EU Directive can potentially interrupt the flow of critical business data, and may expose U.S. companies to prosecution by European authorities for failure to protect the privacy of EU

Safe Harbor

Recognizing the potential impact on trade with EU countries, the U.S. Department of Commerce, in cooperation with the EU, developed a "Safe Harbor" program for U.S. organizations. Through the program, U.S. organizations voluntarily declare certain privacy practices to the Department of Commerce, thereby creating a presumption that they provide a level of "adequate" protection to personal data transferred from the EU.

The Safe Harbor program is designed to bridge the differences between EU and U.S. approaches to privacy protection, and to ensure adequate protection of the personal information of EU nationals. Organizations whose business activities are subject to the jurisdiction of the Federal Trade Commission or the Department of Transportation (the two government agencies that have so far assumed responsibility for monitoring compliance) are eligible to participate in the Safe Harbor program.

To participate in the Safe Harbor program, organizations are required to self-certify annually to the U.S. Department of Commerce compliance with the following seven privacy principles:

Notice. Organizations must notify individuals about the purpose for which they collect and use personal information about them, to whom it is disclosed, and how to contact the organization with inquiries and complaints.

Choice. Individuals must have the option to choose whether their personal information is to be disclosed to a third party, or to be used for a purpose different than that for which it was originally collected or subsequently authorized by the individual. For sensitive information, an affirmative "opt in" choice is required.

Onward Transfer. Organizations must adhere to the notice and choice principles regarding disclosure of personal information to third parties. An organization may transfer information to an outside agent if it makes sure the agent subscribes to the Safe Harbor principles or is subject to the EU Directive or another adequacy finding. As an alternative, a written agreement with the agent must require that the agent provide the same level of privacy protection as is required by the relevant privacy principles.

Access. Organizations must provide individuals reasonable access to their personal information in order to correct, amend, or delete inaccurate information, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy, or where the rights of persons other than the individual would be violated.

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

Data integrity. Personal information must be relevant for the purposes for which it is to be used. And organizations must take reasonable steps to ensure that data collected is accurate, complete, current and reliable for its intended use.

Enforcement. Companies must make available independent recourse mechanisms for complaint and dispute resolution, as well as procedures for verification of adherence to the Safe Harbor principles.

Make Sure Before You Leap

A decision to certify adherence to the Safe Harbor principles is not one to be made lightly. Compliance with these principles requires, among other things, the drafting and implementation of a detailed privacy policy.

Organizations that decide to certify adherence to the Safe Harbor principles, therefore, should make sure that they can meet all of the requirements. Organizations can join the Safe Harbor program via the Department of Commerce's website at www.export.gov/safeharbor, or by sending a self-certification letter. The Department of Commerce maintains a list of all organizations that self-certify and makes the list and related information publicly available on its website.

Once a U.S. organization self-certifies its compliance with the Safe Harbor principles to the Department of Commerce, it is deemed in each EU country to provide "adequate" protection to receive personal information from the EU. In addition, all EU countries will be bound by the finding of adequacy, and any EU country requirements for prior approval of personal information transfers will be either waived or automatically approved.

An organization may choose to withdraw from the Safe Harbor program at any time by notifying the Department of Commerce. Failure to comply with the Safe Harbor principles without officially withdrawing from the program, however, can expose the organization to liability.

In general, enforcement of the Safe Harbor will take place in the U.S. in accordance with U.S. law, and will be carried out primarily by the private sector. An organization that misrepresents its privacy practices in its Safe Harbor self-certification, however, can be subject to prosecution under federal consumer protection laws.

Additional information about the Safe Harbor program, including self-certification procedure, can be found on the Department of Commerce's website, www.export.gov/safeharbor, or the EU Web page on data protection, http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm, also provides helpful information.

Maria E. Recalde is a partner in the Boston office of New Hampshire-based Sheehan Phinney Bass + Green, P.A. She is a member of the firm's business litigation and intellectual property and technology practice groups. She may be reached at mrecalde@sheehan.com.