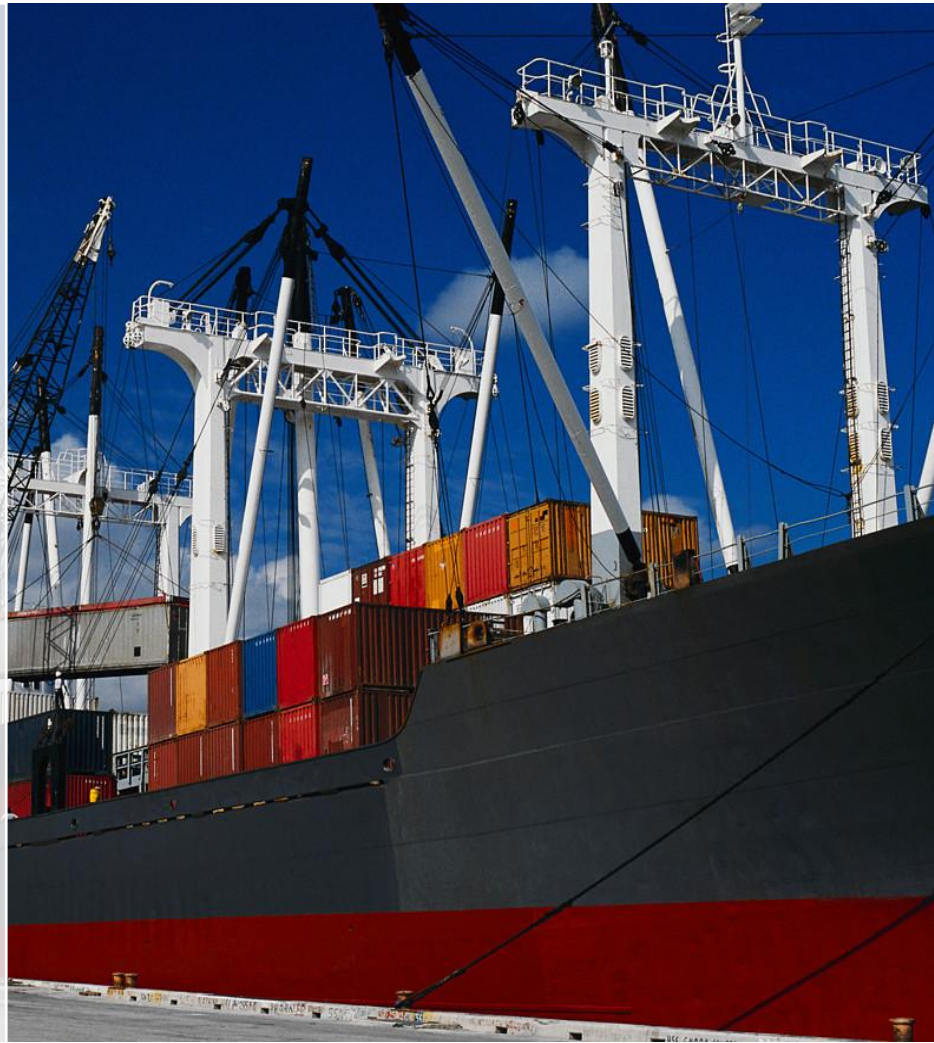


Data Protection in the EU

Jan A. Jensen

2007



Storing data protected by the European data protection laws outside of the EU area can quickly become challenge. Storing personal information about employees or customers in e.g. US is illegal according to data protection laws in most EU countries. But there is a way and it is called the Safe Harbor Agreement.

Z-Solutions GmbH
Lufingerstrasse 13
8185 Winkel
Switzerland
+41 43 422 9334



Data Protection in EU

The Safe Harbor Agreement

Many US based organizations are faced with Safe Harbor requirements when doing business with European companies. At first glance the Safe Harbor Agreement between EU and US looks complicated, but this short step-by-step guide will show that it is easy to get started with.

What is the Safe Harbor Agreement?

Citizens of the European countries are generally speaking very concerned about their privacy and the protection of their personal data. The EU Directive on Data Protection (The 95/46/EC Directive) was agreed to harmonize the rules and regulation on the data protection area in all of the EU member countries. The Privacy Directive requires member countries to pass laws and take steps to protect the private data of their citizens. More importantly the directive directs member countries to prohibit transmission of private personal data to any entity not providing a adequate level of privacy protection.

This directive conflicts with the United States because US, according to the EU does not have adequate privacy protection laws and privacy law enforcement. Until year 2000, there was no agreement between US and EU on how to address this issue and the EU Privacy Directive was threatening to block all transfer of personal data between EU and US, be it customer records, employee data or other kinds of data needed by US companies active in Europe.

Such a situation would have had serious impact on the ability to conduct business across the Atlantic. It was not a desirable situation for neither side and as a result, US and EU started work on a data privacy agreement.

The Safe Harbor agreement was ready in July 2000 and was created to circumvent the negative impact of the directive while providing the EU Citizens with the desired protection of their personal data being transmitted to the US.

The Safe Harbor is a framework providing US companies with a streamlined process to self-certify as complying with the EU Data Protection Directive. A company which wants to certify must comply with seven requirements:

1. Notify individuals about the purposes for which information is collected and used;
2. Give individuals the opportunity to choose (opt-out) of whether their information can 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.
3. Ensure that if the organization transfers personal information to a third party, that the third party also provides the same level of privacy protection
4. The individuals must have access to their personal information in order to correct, amend or delete incorrect information.
5. Take reasonable security precautions to protect collected data from loss, misuse and unauthorized access, disclosure, alteration and destruction.
6. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.
7. In order to ensure compliance with the safe harbor principles, there must be an adequate enforcement mechanism in place.

(Source: U.S. Department of Commerce)

A Safe Harbor certified US company will not have their data flow cut-off by EU data protection regulators except in some special cases where the risk of privacy violations is "imminent" and/or "grave"

What Organizations can or should join the Safe Harbor Agreement?

Any US organization which receives any kind of personal information or pieces of information which can be used to identify a unique EU individual be it phone numbers, banking information, social security numbers, Identity number or any kind of address information are required to demonstrate that they provide adequate privacy protection.

A US organization which receives such information should consider joining the Safe Harbor agreement to demonstrate compliance with the EU Data Protection directives adequacy requirement.

Any U.S. organization that is subject to the jurisdiction of the Federal Trade Commission (FTC) or U.S. air carriers and ticket agents subject to the jurisdiction of the Department of Transportation (DoT) may participate in the Safe Harbor. 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 Safe Harbor framework but then fail to live up to their statements.

Source: US Federal Trade Commission

What are the advantages of joining the Safe Harbor Agreement?

Some EU based organizations are bared from transferring personal information outside the EU unless they at least are able to provide proof of the receiving organization providing adequate data protection.

The Safe Harbor agreement eliminates the need for prior approval to begin data transfers to the US or it gives an automatic approval because US organizations under the Safe Harbor Agreement are deemed adequate. The enforcement will be conducted in the United States instead of in Europe subject to some limited exceptions.

The Safe Harbor agreement provides the EU based organization with the needed confirmation with regards to adherence to EU and national data protection laws and regulations. Finally, the agreement binds all EU Member States to the European Commission's finding of adequacy.

How can organizations join the Safe Harbor Agreement?

The process to join is actually relatively simple. Any organization wanting to join should go through these steps:

1. Develop a privacy policy compliant with the seven privacy principles in the Safe Harbor agreement (see above) Notice, Choice, Onward Transfer, Security, Data Integrity, Access & Enforcement
2. Implement mechanisms enforcing the privacy policy such as encryption of data stored, customer access, opt-out features etc.
3. Implement the required mechanisms for dispute resolutions, verification of adherence to the seven privacy principles and mechanism to rectify problems arising out of a failure to comply with the principles including adequate sanctions.

4. Clearly state on company web page and in privacy policy that the organization adheres to the Safe Harbor Agreement
5. Fill out the certification form and submit it (can be done online) to US Department of Commerce

The verification process

The required verification can be carried out by either Self-Assessment or by Outside Assessment. The selected method has to be clearly indicated in the published privacy policy. The purpose of the process is to verify that the US Organizations privacy policy regarding personal information received from the EU conforms to the Safe Harbor Principles, that it is being complied with and that individuals are informed of the mechanisms through which they may pursue complaints

The assessment has to be conducted once per year and should be signed by either a corporate officer or by the reviewing outside assessor.

Nothing speaks against conducting the assessment internally in the organization, but outside assessments are normally more respected and trusted.

The verification process can include but is not limited to privacy audits, random reviews or the use of honey pots.

It should be noted that the EU states that companies transferring employee and salary information to the US are obligated to make their Employee Privacy Policy public in the same way as other organizations. An internal privacy policy published in the employee handbook is not compliant with the Safe Harbor agreement – This has however been disputed by US officials from the US department of Commerce stating that as long as the Employee Privacy Policy is freely available internally, it does not have to be made public.

© 2007 Jan A. Jensen, Z-Solutions GmbH. All rights reserved

About the Author:

Jan Anker Jensen has more than 16 years of international experience as senior manager, project- & programme manager and consultant in the Customer Care-, ICT-, Financial Services- , Hi-Tech-, Telecommunication- and Outsourcing industry.

In 2002 he established Z-Solutions GmbH (Pronounced: See-Solutions).

About Z-Solutions GmbH

Z-Solutions was established in 2002 and has since consulted companies like o2 Mobile, Orange Business Services, Zurich Financial Services, Nokia, Swisscom and many others worldwide.

The company is focused on helping customers in the areas of strategy, management, technology and performance in the following industries: Customer Care-, ICT-, Financial Services- , Hi-Tech-, Telecommunication- and Outsourcing industry.

Z-Solutions offers the following services: Consulting, Project- & Programme Management, Interim Management and Coaching.