THE END OF SAFE HARBOR!
WHAT HAPPENS NEXT?
Sending data from the EU to the US is no longer a walk in the park! On October 6, 2015, the European Court of Justice announced that the Safe Harbour has been ruled as invalid.

What is Safe Harbour?

Safe Harbour is a pact that was established in 2000, to allow US companies get data from Europe in a cost-effective way. Since data transferring outside EU countries has been limited by the EU Data Protection Directive, this pact was agreed by US and Europe, to allow organizations do this in a quicker way, without breaking the rules.

However, this pact was contested last year when the privacy campaigner, Max Schrems, required information on how data are being processed by Facebook. After his requests were denied, he referred this case to the European Court of Justice, to review the safe harbour pact, and whether data and privacy of information are protected properly through this pact. Therefore, the European Court of Justice decided on October 6, that the pact is invalid, and every US firm who receives data from Europe, has to go through the compliance and documented procedures to ensure that they are taking adequate data protection measures.

How will this affect US firms?

Knowing that there are more than 5000 companies which were relying on the Safe Harbour agreement, the outcome of this decision is expected to be significant, because of the relevant implications related to EU based companies that share data with organizations based in North America. The real outcome of this decision will affect all organizations that process or store data about European citizens. Every organization that sends payrolls, personal information, marketing campaign information, customer data, financial information, etc. is responsible for ensuring that the US recipient fully meets the eight Data Protection Principles of the EU Directive.

In order to fulfill these obligations, US organizations may need to implement additional layers of security to protect this data and uphold the citizen’s right to privacy. As Allie Reninson from the UK’s Institute of Directors stated in an interview with the BBC, “It’s not just about companies whose core activities are data processing - i.e. the Facebooks of the world - it’s the companies who don’t have data processing capabilities of their own and transfer personal data abroad to get it done.”
What happens next?

A pragmatic solution to this problem is utilizing internationally recognized standards, which provide documented procedures that provide control and assurance in relation to data protection and privacy.

An internationally accepted approach is outlined in ISO/IEC 29100, which was developed by the International Organization for Standardization in 2011, as a way to provide organizations with instructions on how to specify, define, architect, design, develop, test, maintain, administer and operate information and communication technology systems or services where privacy controls are required for the processing of Personally Identifiable Information (PII).

ISO/IEC 29100:2011 provides a privacy framework which:
- specifies a common privacy terminology;
- defines the actors and their roles in processing personally identifiable information (PII);
- describes privacy safeguarding considerations; and
- provides references to known privacy principles for information technology.

What does all this mean?

This means that organizations around the world need to embrace procedures and actions to ensure that privacy is respected and data are protected. Becoming aligned to ISO/IEC 29100 is an essential step towards organizations around the globe being able to fulfill a variety of international legal and regulatory requirements. The implementation of such a framework will go a long way towards supporting organizations on both sides of the Atlantic.

In response to this, PECB has developed a 5 day Certified Lead Privacy Implementer training course with certification, for all professionals who want to develop the necessary expertise to support an organization in implementing and managing a Privacy Framework based on ISO/IEC 29100, the Generally Accepted Privacy principles and guidance from international information commissioners.

Considering that the demand for compliance to ISO/IEC 29100 is likely to increase rapidly worldwide, professionals looking to benefit from this change need to consider this course and become certified to help organizations embrace this proven standard.

For further information, please visit the PECB website and refer to the Certified Lead Privacy Implementer course brochure.