Safe Harbor and GDPR Action Plan

On Oct 6 2015, the European Court of Justice (ECJ) – Europe's highest court – concluded that the US-EU Safe Harbor agreement between the European Commission and the U.S. Department of Commerce was invalid.

In addition, many observers expect the EU will soon adopt the General Data Protection Regulation (GDPR) with a two-year grace period for compliance. The GDPR will apply not only to businesses based in the EU, but also to businesses outside the EU that process personal data collected through offering services or goods to citizens in the EU, from monitoring their behavior, or hosting their data.

Why should US Companies Act?

- Companies face legal risk if they do not put in place a valid mechanism for transferring personal data to the U.S.
- Non-compliance with GDPR may result in substantial new penalties of up to €100 million, or 2-5% of annual worldwide turnover, whichever is greater.

EU data-transfer mechanism status tracker

The EU's decision to invalidate Safe Harbor is having a domino effect on the other acceptable data-transfer mechanisms, causing the need for U.S. companies to monitor their status.

Mechanism	Status	Outlook
EU-US Safe Harbor	Invalidated by the European Court of Justice. The Article 29 Working Party has concluded data transfers relying on Safe Harbor are unlawful.	Legal experts say a US-EU treaty would be needed to establish a truly robust new version of the Safe Harbor. Current negotiations are underway but the outcome is uncertain.
Swiss-US Safe Harbor	Switzerland said it would follow the EU's direction.	
Binding Corporate Rules (inc. BCR for Processors)	Article 29 Working Party has indicated it will be analyzing the impact of the ECJ decision on all other data-transfer mechanisms. German data-protection authorities have suspended BCRs and BSPRs for transfers to the U.S.	The legal precedent set by the European Court of Justice in its Safe Harbor ruling has called into question the long-term viability of these options.
Model Contracts, approved by the European Commission	German data-protection authorities have said they may fine U.S. companies not in compliance with their model clauses. Belgium's high court has approved fining of a U.S. company for alleged noncompliance.	
Data-subject consent	EU data-protection authorities have not changed their limited support for this mechanism.	The difficulty of getting consent for large classes of people will continue to make this option impractical for many companies.

The challenges for US businesses are these: what do good privacy programs look like and how they prove that their program s are good?

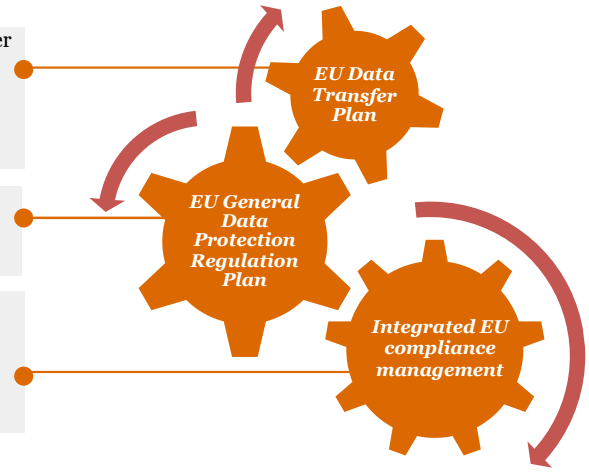
"Operational Adequacy Schemes" - Your Action Plan

U.S. companies with operations in Europe may wish to consider adopting the action plan outlined below.

- **Assess personal data flows** from EU-to-US to define the scope of the crossborder privacy compliance challenge.
- **Assess model contracts** as at least a temporary replacement to Safe Harbor.
- **Assess readiness** to meet model clauses, remediate gaps, and organize audit artifacts of compliance with the clauses.

- **Conduct** a GDPR readiness assessment.
- **Budget** for GDPR remediation.
- **Elevate** risk and mitigation plans to the Board level.

- **Enhance** your EU privacy program to ensure it is capable of passing an EU regulator audit, or litigation challenge, remediating GDPR gaps along the way.
- **Conduct** EU data-breach notification stress tests.
- **Monitor** changes in EU support for model contracts and binding corporate rules and prepare to shift to the operational adequacy mechanism.



Assess your overall 'Operational Adequacy' to meet multiple and varied requirements on an ongoing basis.

pwc

For further information please contact:

Stewart Room
Partner, Cybersecurity and Privacy, PwC Legal LLP
stewart.room@pwclegal.co.uk
http://pwc.blogs.com/data_protection/