Differing local privacy and data protection laws, especially in the EU, have increasingly challenged U.S. cloud providers seeking to move and store data across the globe. New guidance and public statements by the United States Department of Commerce come at an important time, as privacy and data protection issues increasingly derail and slow transactions involving U.S. businesses seeking to do business online and abroad.

Online businesses recently have encountered resistance and skepticism about the U.S.-EU Safe Harbor (“Safe Harbor”) program and its efficacy in meeting EU requirements. The Safe Harbor program allows U.S. organizations to lawfully receive, maintain, and process personal data about data subjects located in the EU. According to the Commerce Department’s announcement in April 2013, cloud providers in the United States satisfy the EU’s data protection requirements for data transfers when they adhere to the Safe Harbor. The Commerce Department concluded that cloud computing does not differ from any other type of data processing, and it maintained that the Safe Harbor’s flexibility can account for any potentially unique issue that may be raised by cloud computing.

The Article 29 Data Protection Working Party prompted the Commerce Department’s announcement when its opinion on cloud computing suggested that entities in the EU may not be able to rely solely on the Safe Harbor to lawfully transfer personal data to U.S.-located cloud providers. The Working Party is an independent advisory body on data protection and privacy issues comprised of representatives from each European data protection authority, the European Commission, and the European Data Protection Supervisor. Its opinions are not binding and do not constitute legal requirements, but they are highly persuasive for EU data protection authorities and courts and thus should be taken into account by entities doing business in the EU.

**European Commission’s “Adequate” Data Protection Findings.** The EU’s Data Protection Directive 95/46/EC (EU Directive) prohibits data transfers out of the EU to other countries unless the personal data is sent to a country that the European Commission (EC) recognizes as providing “adequate” data protection. At this stage, the EC has recognized only a small number of countries as providing an adequate level of protection. The U.S. has not yet been deemed adequate under EU law. Even if a country does not provide adequate data protection, the EU allows entities within those countries to ensure adequate data protection by using contractual methods, such as approved standard contractual clauses (“model clauses”) or Binding Corporate Rules (BCRs).

Companies may also rely on consent from the data subjects, but obtaining consent can often be difficult to achieve and may be more restrictive than many U.S. companies expect. Many organizations have concluded that aspects of model clauses and BCRs provide less-than-satisfactory solutions over time.

**The Safe Harbor.** Due to the importance of global trade between the EU and the U.S., the EC and the U.S. negotiated an agreement to help ensure the continued free flow of protected personal information between the regions. Under the Safe Harbor, which the EC and European Economic Area officially recognized as ensuring adequate data protection, U.S. organizations that affirmatively commit to adhere to the Safe Harbor Privacy Principles obtain the benefits of the safe harbor.

Despite the clear purpose and adequacy of the Safe Harbor, many U.S. organizations have encountered difficulties in business negotiations and contract negotiations when interacting with third parties in the EU, especially those located on the continent. The Commerce Department countered four primary concerns about cloud computing and the Safe Harbor program raised by the Working Party’s opinion.

---

1. Safe Harbor Certification Alone Is Sufficient for Lawful Data Transfers.

---


3 The adequacy decisions of the European Commission are binding upon all EU countries.
Perhaps of most concern to cloud providers was the Working Party’s suggestion that Safe Harbor-certified U.S. cloud providers have additional requirements that other types of entities do not have when working with personal data from the EU. The Working Party suggested that customers of cloud providers (“cloud customers”) should require cloud providers, even those that are Safe Harbor certified, to agree to contracts compliant with the different EU Member States’ data protection requirements, or to use another data transfer mechanism such as standard contractual clauses or BCRs. The Commerce Department reiterated that the European Commission recognized that the Safe Harbor program guaranteed adequate data protection. Therefore, the Safe Harbor is a complete safe harbor. As the Commerce Department stated, “Additional requirements cannot be imposed exclusively on U.S. service providers processing personal data transferred from the EU . . . because they satisfy the ‘adequacy’ requirements through Safe Harbor certification.”

2. Certified Cloud Providers and Their Subcontractors Are Required to Provide Data Protection Deemed Adequate by the EC. The Working Party also expressed concern with the lack of transparency regarding cloud providers’ use of subcontractors and the data protection provided by those subcontractors. The Commerce Department stated that the Safe Harbor requires cloud providers to use either subcontractors located in countries deemed adequate by the EC or contractually require their subcontractors to provide the same level of data protection as is required by the Safe Harbor Privacy Principles. Therefore, when cloud customers do business with a Safe Harbor-certified cloud provider, the cloud provider and any entities processing the data on its behalf are required to comply with the Safe Harbor Privacy Principles, which presume that any specific local EU data protection requirements also will be satisfied.

3. Security Requirements of Safe Harbor Consistent with EU Directive. The Working Party also was dismayed that the Safe Harbor does not explicitly address cloud-specific security risks. Both the EU Directive and the Safe Harbor are designed to be flexible, technologically neutral, and principles-based, and defining specific security safeguards does not seem in line with those goals. The Commerce Department maintains that the Safe Harbor requires “reasonable precautions,” which is similar to the EU Directive’s requirement of “appropriate technical and organizational measures” and consistent with EU data protection law. Under the Safe Harbor Security Principle, the cloud customer and cloud provider are responsible for contractually defining the specific security requirements that provide “reasonable precautions.”

4. The Commerce Department Maintains a Public List of Organizations That Have Self-Certified to the Safe Harbor Framework. The Working Party encouraged cloud customers to verify the Safe Harbor certification of cloud providers and perform additional due diligence regarding compliance. The Commerce Department provides a website for cloud customers to verify a cloud provider’s certification to the Safe Harbor. The website also allows cloud customers to review the information submitted as part of the self-certification process, such as the organization’s privacy policy. In practice, many businesses increasingly perform additional due diligence to review privacy and data protection compliance with potential vendors and service providers.

Cloud providers may have been taken aback by the Working Party’s opinion, and they faced increasing pressure from cloud customers to respond to the Working Party’s concerns. In its recent announcement, the Commerce Department strongly defended the Safe Harbor program as a mechanism to ensure adequate data protection, even as applied to cloud providers. The Commerce Department’s guidance strongly suggests that U.S. cloud providers should not be singled out as entities that must provide additional assurances to cloud customers in the EU before maintaining personal data for them. Instead, the Commerce Department maintains that cloud customers should feel confident that Safe Harbor-certified cloud providers provide adequate data protection as required by the EU Directive.

Implications

The Commerce Department’s strong support of the Safe Harbor program suggests the ongoing value and benefit to U.S.-based enterprises seeking to ensure adequate data protection of personal information processed from the EU. Entities that choose to participate in the Safe Harbor must, among other requirements:

1. self-certify annually to the Safe Harbor Framework’s requirements, which include elements such as notice, choice, access, and security;
2. adhere to such requirements;
3. verify adherence using a self-assessment or a third-party assessment.

---

1 The Commerce Department actively works to resist trade restrictions that might discriminatorily impact U.S. cloud providers. However, the presence of “local” data protection requirements, which typically may be found in data protection agreements expected of processors, persists. Given that many data protection authorities accept model clauses as a substitute for such agreements, U.S. Safe Harbor adherents—in particular, EU member states—will likely in the near term continue to be forced to examine their contracts to provide services. These reviews may lead to the inclusion of specific amendments and addendums or execution of model clauses to address additional specific local requirements.

program; and

4. state in their published privacy policy statements that they adhere to the Safe Harbor Privacy Principles.

The Federal Trade Commission (FTC) may take enforcement action against entities that publicly state that they are in compliance with the U.S.-EU Safe Harbor Framework but fail to live up to their statements. Under Section 5 of the Federal Trade Commission Act, for example, an entity’s failure to abide by commitments to implement the Safe Harbor Privacy Principles might be considered deceptive and actionable by the FTC.

While completing the required Safe Harbor application is relatively simple and quick, it can be easy for organizations to overlook the program’s compliance requirements, including annual assessments and documentation of compliance. Given the increasing attention and focus by customers on vendor and supply chain management in this area, increased investment in privacy and data security-related controls may yield quick returns by enabling deals to close more quickly and efficiently. Moreover, with the FTC’s prosecution of a number of entities that claimed they were Safe Harbor-certified even though their certifications had lapsed, technical compliance with the Safe Harbor has taken on greater significance. A benefit of the program is that it helps encourage organizations to routinely and annually re-evaluate their privacy and data protection practices and to do so systematically. Many organizations also rely on and work with outside third parties, including law firms, to assist in these efforts. Such assistance can provide valuable benchmarking information and guidance on best practices, as well as assist with risk management.

Wilson Sonsini Goodrich & Rosati’s privacy and data security practice routinely advises clients on privacy and data security matters, including compliance with EU privacy or data protection legislation and the U.S.-EU Safe Harbor Framework. The firm also regularly assists companies with all legal aspects associated with the collection, use, and disclosure of personal data globally. For more information on our privacy and data security practice, please visit http://www.wsgr.com/WSGR/Display.aspx?SectionName=practice/privacy.htm. For additional information, please contact Gerry Stegmaier at gstegmaier@wsgr.com or (202) 973-8809, Cédric Burton at cburton@wsgr.com or +32 2 274 57 22, Wendell Bartnick at wbartnick@wsgr.com or (202) 973-8963, or any member of the privacy and data security practice.