D&G | Davis & Gilbert LLP
ATTORNEYS AT LAW

NOVEMBER 2011

ADVERTISING, MARKETING & PROMOTIONS

>> ALERT

FTC ENDORSES NEW PRIVACY SYSTEM FOR THE UNITED STATES AND ASIA-PACIFIC REGION REGARDING CROSS-BORDER DATA TRANSFERS

Cross-border data transfers have become increasingly complex over the years as different countries and regions enforce privacy laws and practices that vary from those in the United States.

NEW APEC SELF-REGULATORY PRIVACY INITIATIVE

With the hope of easing the burden on U.S. businesses, the Federal Trade Commission (FTC) this month endorsed a new program by the Asia-Pacific Economic Cooperation (APEC) to unify cross-border data privacy protection among members of APEC. APEC is a forum for 21 member Pacific Rim countries (member economies) which seeks to promote free trade and economic cooperation throughout the Asia-Pacific region. In light of a continual increase in the amount of consumer information moving across national borders, APEC's program is designed to enhance the protection of consumer data that flows between the United States and other APEC member economies. The FTC and the Department of Commerce assisted in the development of the new APEC privacy program.

Companies that wish to participate in the APEC privacy system will undergo a review and certification process by third parties that will examine corporate privacy policies and practices and enforce the new initiative privacy rules.

The 21 APEC members who will participate in this program are Australia, Brunei, Canada, Chile, China, Hong Kong, Indonesia, Japan, Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, the Philippines, Russia, Singapore, Taiwan, Thailand, and Vietnam.

APEC member economies expect to launch the new privacy system next year.

COMPARISON TO THE U.S.- EU SAFE HARBOR PROGRAM

This new privacy initiative is certainly not the first cross-border privacy regime. The U.S.-EU Safe Harbor Program administered by the U.S. Department of Commerce has been in effect for a decade serving to bridge the differences between U.S. and EU privacy regimes. The European Union

>> continues on next page

THE BOTTOM LINE

The APEC privacy program is a self-regulatory regime designed to create more consistent privacy protections for consumers when their data moves between APEC member economies that have different privacy regulations. As more and more consumer information is transferred around the world, differences in the privacy regulations of various regions highlight the need for compliant cross-border data practices. If your business involves moving consumer data across borders, it is imperative to have privacy practices that comply with all applicable foreign requirements.

has privacy legislation which is regarded as more centralized and rigorous than that found in many other areas of the world, including the United States. Personal information of EU residents may only be transferred out of the EU to countries which have adequate privacy protections. Since the United States is considered by the EU to have inadequate privacy protections, the Safe Harbor Program was put in place. Once a U.S. company has joined the Safe Harbor program, it is deemed to have adequate privacy protections and is eligible to receive personal information of EU residents. There are other methods to meet the EU's requirements but the Safe Harbor Program is a popular and beneficial method. U.S. companies can opt into the Safe Harbor Program, provided that they adhere to the seven principles outlined in the EU Directive on the Protection of Personal Data. The seven principles are as follows:

- **Notice** - Individuals must be informed that their data is being collected and about how it will be used.
- **Choice** - Individuals must have the ability to opt out of the collection and forward transfer of the data to third parties.
- **Onward Transfer** - Transfers of data to third parties may only occur to other organizations that follow adequate data protection principles.
- **Security** - Reasonable efforts must be made to prevent loss of collected information.
- **Data Integrity** - Data must be relevant and reliable for the purpose it was collected.
- **Access** - Individuals must be able to access information held about them, and correct or delete it if it is inaccurate.
- **Enforcement** - There must be effective means of enforcing these rules.

After opting in, an organization must re-certify every twelve months. The company can either perform a self-assessment to verify that it complies with these seven principles, or hire a third-party to perform the assessment. Additionally, there are requirements for ensuring that appropriate employee training and an effective dispute resolution mechanism are in place.

FOR MORE INFORMATION

Gary A. Kibel
Partner
212.468.4918
gkibel@dglaw.com

Alison Winter
Associate
212.468.4976
awinter@dglaw.com

or the D&G attorney with whom you have regular contact.

Davis & Gilbert LLP
T: 212.468.4800
1740 Broadway, New York, NY 10019
www.dglaw.com