Central American Data Privacy Updates

1. Costa Rica

On March 5, 2013, Costa Rica’s data protection law, originally passed in 2011, came into force. The law, the Ley Protección de la Persona frente al tratamiento de sus datos personales, Law 8968, requires explicit data subject consent for any processing of data. Under the March 5 regulations implementing the law, companies must notify data subjects within five days of any “irregularity in the processing or storage of their data,” such as a data breach or theft. Companies must also notify the Costa Rican data protection authority, the Agencia de Protección de Datos de los habitantes (“Prodhab”), of any data breach.

South American Data Privacy Updates

1. Colombia

On April 18, 2013, Colombia’s data protection law, Ley 1581 del 17 de Octubre de 2012 por el cual se Dictan Disposiciones Generales para la Protección de Datos Personales, took effect. In late June 2013, implementing regulations for the law were published by the Colombian government. The law was initially passed on October 17, 2012 with a six-month grace period for companies to come into compliance. Among its chief provisions, the law requires that data subjects give prior, informed consent before any collection occurs. The law also restricts processing of sensitive data without consent to just a few limited circumstances, such as those situations when processing is required by law. The implementing regulations impose fines of more than $600,000 for non-compliance.

2. Peru

On March 22, 2013, Peru’s Personal Data Protection Law took effect – 30 days after the Peruvian government published implementing regulations for the law. While Peru’s law does not require notification to any central authority or data subject in the event of a breach, the law generally requires data subject consent to process data. Further, the law provides individuals with various rights to access, update, or eliminate personal data held on
them by a company. The implementing regulations clarified several aspects of the legislation, including registration of databases with the National Register of Personal Data Protection and enforcement.

3. Uruguay

On April 12, 2013, Uruguay acceded to the European Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108) and its Additional Protocol. Uruguay was the first non-European country to accede to the convention, perhaps signaling the growing influence of the European Union on data privacy issues. This event comes on the heels of the European Commission’s declaration last year that Uruguay’s data protection regime was adequate under the European Data Protection Directive. Data privacy in Uruguay is governed by the Protection of Personal Data and “Habeas Data” Action 18.331 (“PDHDA”), which was passed in 2008.

4. Brazil

In Brazil, the “Marco Civil” has become a priority for the Brazilian government in late-2013 following Edward Snowden’s revelation of the NSA’s PRISM program. The Marco Civil is aimed at defining core rights of the Internet—including freedom of access, expression, privacy, and data protection. However, recent amendments to the Marco Civil added after the NSA PRISM scandal broke may also have serious implications for companies doing business in Brazil. These amendments would require companies to use local data storage centers to store data on their Brazilian users. Companies could not transfer personal information of Brazilians outside of Brazil for storage or processing. Google recently spoke out against the proposed change to the Marco Civil, stating: “The proposed amendment requiring internet companies to store Brazilian user data in Brazil risks denying Brazilian users access to great services that are provided by U.S. and other international companies.”

In addition to the Marco Civil, the Data Protection Bill of 2011 may still be considered by the Brazilian government in 2014. This draft legislation would establish a Data Protection Authority, require data subject consent prior to transfers of data, and require data breach notification.