Latin America is in the summer spotlight with the hosting of the International Olympic Games in Brazil and the 100th anniversary of the Copa América futbol tournament, making this a timely moment to take stock of where data privacy regimes stand in Latin America.

Latin America is not a monolith, the region is comprised of a multiplicity of languages, cultures and privacy laws. Given the absence of any omnibus regional law or EU-like set of directives, companies must assess their business models and data monetization strategies in the context of each country’s framework.

This note provides an overview of some of the key privacy themes and differences across the region for enterprises considering their involvement in these developing markets.

Data Protection in Latin America

Broadly speaking, Latin American nations’ approach to data protection fall into the following four groups:

- **Constitutional/Habeas Data.** Nations which utilize a constitutional rights-based model for protecting individuals’ personal data rights
- **General Data Protection Laws.** Nations which have enacted comprehensive data protection laws
- **Hybrid Approach.** Nations that employ a blend of habeas data and general data protection laws
- **Unsettled or Transitioning Data Protection Rights.** Nations that lack a clearly defined constitutional or legislative structure with respect to privacy rights.

Please note that this memorandum is intended as a general overview of the subject and cannot be regarded as legal advice.
While no country’s data protection framework fits neatly into a single silo, broadly speaking, Latin American nations’ frameworks fall into the following four groups:

- **Constitutional/Habeas Data.** Nations which utilize a constitutional rights-based model for protecting individuals’ personal data rights, exercisable through legal action and further interpreted within the court system, include: Brazil, Chile, Ecuador, Honduras, Panama and Paraguay

- **General Data Protection Laws.** Nations which have enacted comprehensive data protection laws that codify elements such as notice, choice, access, correction, breach notification, and data retention requirements include: Costa Rica, Mexico, Nicaragua and Uruguay

- **Hybrid Approach.** Nations that employ a blend of habeas data and general data protection laws (i.e., those that complement constitutional protections with expansive data protection legislation) include: Argentina, Colombia and Peru

- **Unsettled or Transitioning Data Protection Rights.** Nations that lack a clearly defined constitutional or legislative structure with respect to privacy rights, or that do not currently have a supervisory data protection authority in place, include: Bolivia, El Salvador, Guatemala and Venezuela
LATIN AMERICAN PRIVACY REGIMES: NATIONS AT A GLANCE

Argentina

Argentina’s comprehensive data protection law, passed in 2000, provides general protection for personal data stored in public or private databases and other processing platforms, just as Chapter VII of the Federal Constitution recognizes individuals’ habeas data rights to access and correct information stored about them. Moreover, it is a crime punishable by prison to knowingly insert false information into a personal data file.

In addition to enforcing laws recognizing “network neutrality” and the regulation of IT and communication services, Argentina’s DPA is highly proactive. In April 2016, it forced a U.S.-based ride-sharing service to take down its website and mobile apps in-country as part of a privacy law compliance investigation. In May 2016, the DPA issued an open consultation to further modernize its privacy law in response to technological advances.

Brazil

Brazil, one of the so-called “BRIC” emerging economies, presently lacks a comprehensive data protection law or a national DPA. Instead, personal data protections derive from the Brazilian Constitution—which treats privacy as inviolable and recognizes habeas data— Consumer Codes, and certain sector-specific laws that have privacy as a component. The civil court system provides the most frequent avenue for redress of privacy grievances.

The enactment of a 2014 Internet “civil bill of rights,” which applies to broadband providers, social media sites, search engines and other online hosting providers, reflects a trend in Brazilian data privacy rights being more broadly applied, by prohibiting the sharing of users’ personal data with third parties without express consent. A bill circulating in Congress provides for encryption, data minimization rules and definitional clarifications of “personal data,” but experts are skeptical as to any immediate timeframe for its passage.

Chile

Although Chile is credited with enacting the first Latin American privacy law in 1999, in its present form the Chilean law is anemic in its actual protections. The law nominally regulates the processing of individuals’ personal data, but lacks provisions restricting international personal data transfers, creation of a DPA, or appointment of a DPO.

To remedy the perception of being privacy-deficient, lawmakers are engaged in a major revamp of the law to impose data breach sanctions, require database registrations, and establish a DPA, which is seen as a prerequisite for Chile being deemed “adequate” to compete for Spanish-language services outsourced from the EU.

Colombia

Colombia’s data privacy regime has been upscaling since a 2008 law addressing personal data use in financial industries. In 2012, a comprehensive law was enacted that provided for data protections in the public and private sectors, and was bolstered in 2013 by decrees involving data subjects’ rights, treatment of sensitive data, and cross-border transfers. The Constitution’s Article 15 provides for habeas data and the right to personal and family privacy, including for collection and storage of data, which the courts have further defined.

Costa Rica

Costa Rica’s general data protection law, which came into full effect in 2011 and was expanded in 2013, requires the informed consent of data subjects before personal data can be collected or transferred, and sets various security mechanisms and safeguards for sensitive data. The law applies to all processing of personal data by both public and private entities. A unique feature is Costa Rica’s superusuario requirement whereby the DPA must be provided a user profile allowing for unrestricted access to registered databases.
LATIN AMERICAN PRIVACY REGIMES: NATIONS AT A GLANCE

Mexico

Mexico’s 2010 enactment of a federal data protection law solidified a system for regulating the processing and protection of data stored by private entities. The law was enhanced in 2013 with guidelines relating to different forms of privacy notices (i.e., notices of varying levels of specificity—comprehensive, simplified or short—depending on the context).

Mexico’s DPA’s profile has risen in recent years, with headline-grabbing enforcement fines and other efforts to differentiate its approach to privacy compared to counterparts. In June 2016, the DPA announced a contest to “identify, publicize and disseminate, nationally and internationally, the best practices for the protection of personal data occurring in Mexico.”

According to news reports, an even more robust privacy bill may circulate in Mexico before the end of the year, which could contemplate, for instance, data portability obligations, employee privacy rules, and extra-territorial jurisdiction over non-local data processors.

Nicaragua

Nicaragua’s 2012 national data protection law and regulations protect the personal data of individuals that are stored in private and public databases. Unlike many countries, Nicaragua’s law includes a “right to be forgotten,” such that individuals have the right to request that search engines and social media sites remove their personal data from databases (though the record is unclear as to whether or how this has been challenged).

Peru

Peru’s constitution and national data protection law, which was enacted in 2011, recognize habeas data and guarantee the fundamental right to protection of personal data processed in the public and private sectors. Peru’s law mandates special rules for the processing of minors’ personal data, and the DPA has held that all information that users of any age publish on social media profiles is considered private and thus cannot be used by others without consent. Peru is both an APEC economy and a Trans-Pacific Partnership signatory.

Uruguay

Uruguay, the other Latin American nation (along with Argentina) to be recognized as providing an adequate level of protection for transfers of personal data from the EU, has a data privacy regime that recognizes that the protection of personal data is fundamental to the human experience. To that end, its national data protection law, which incorporates habeas data provisions, applies to personal data stored on any processing platform.
CENTRAL THEMES IN LATIN AMERICAN PRIVACY FRAMEWORKS

Data Protection Authority (DPA) Registration Requirements
Whereas neither Mexico nor Nicaragua requires businesses to register with the respective DPAs, in Peru, all organizations must register with the DPA. Argentina, Costa Rica and Uruguay generally require organizations to register their databases in order to process personal data. In Colombia, not only must businesses that process personal data register with the DPA, but so too must service provider processors.

Adequacy and Cross-Border Data Transfer
Argentina (which requires encryption for sensitive personal data to be transferred), Colombia, Nicaragua, Peru and Uruguay prohibit the transfer of personal data to countries and/or recipients that do not provide an adequate level of protection—for which the DPAs do not provide an approved list. For countries not deemed “adequate” to the transferring nation’s standards, other transfer mechanisms usually exist, such as contractual provisions and data subject consent.

Two Latin American nations have been deemed to provide a level of protection “essentially equivalent” to the EU: Argentina in 2003 and Uruguay in 2012.

DPA Enforcement
Neither Brazil or Chile currently have a DPA, however discussions on a Chilean data protection law overhaul are said to envision a robust regulator. Nicaragua has a DPA provided for in its national data protection law, but an agency has yet to be formally established. Peru’s DPA has begun to flex its punitive muscles by fining online and marketing companies that publish sensitive personal data without the subjects’ consent. Mexico’s DPA has been forceful in fining privacy violations, including against banks and mobile carriers.

Asia-Pacific Economic Cooperation (APEC)
APEC, a collection of more than twenty regional economies that seeks to promote growth and harmonize interoperability among varied legal systems, endorsed in 2011 its Cross-Border Protection Rules (CBPRs) to allow the transfer of personal data among member economies who implement privacy practices consistent with the APEC Privacy Framework.

At present, three Latin American nations—Chile, Mexico and Peru (host of a 2016 APEC summit), each of which is also a signatory of the Trans-Pacific Partnership (TPP)—are APEC members and will surely inspire neighbors to likewise join and establish new trade opportunities.

Data Security
Whereas Brazil and Chile have no generally applicable data security standards, Argentina has adopted a layered set of database security requirements based on risk profile and the types of data involved, while Mexican regulations more prescriptively set security protocols and monitoring, training and auditing requirements. On the other end of the spectrum is Nicaragua, which lacks specific data security requirements.

Data Breach Notification
In Colombia, whereas businesses are required to inform the DPA of possible data incidents, there is presently no requirement to notify affected individuals of breaches. Conversely, in Mexico the discovery of a data breach that could materially affect personal or property rights must be reported to the individual (as is the case in Uruguay), but not the DPA. Whereas Argentina, Brazil and Chile do not mandate notification, Costa Rican law requires that subjects be informed of processing “irregularities” within 5 business days of discovery.

Appointment of a Data Protection Officer (DPO)
Organizations are required to designate a privacy officer or other individual who will be accountable for the privacy practices of an organization in Colombia and Mexico. This is in contrast to, for instance, Chile, Nicaragua and Uruguay, which do not require a DPO.

The Right To Be Forgotten (RTBF)
Several nations, including Costa Rica, Nicaragua and Uruguay, explicitly recognize the RTBF (whether in actual legislation or in jurisprudence), primarily in relation to financial and criminal matters. Whereas Colombia’s Constitutional Court adopted a similar right, Argentina’s Supreme Court refused to recognize the RTBF in a 2014 case involving the unauthorized commercial use of an individual’s image available via search engines.
**KEY TAKE-AWAYS FOR COMPANIES SEEKING TO COMPLY WITH LATIN AMERICAN PRIVACY REQUIREMENTS**

- Latin America is as diverse in its privacy regimes as it is in its geographies. Rather than adopting a regional approach, before operationalizing businesses must have an exemplary grasp not just of the local rules but also of their global data flows—which can be clarified via TRUSTe’s Consulting Services and Assessment Manager platform.

- Habeas data is a constitutionally-based remedy of legal action that may be initiated by a citizen to discover what data is held about that person, in order to facilitate correction or deletion of the information.

- More incentives than ever exist for Latin American governments to modernize their data privacy laws in light of APEC membership, global commerce and trade, and international adequacy/interoperability opportunities. With Chile, Mexico and Peru already APEC members, companies should consider APEC CBPR Certification as a route to demonstrate compliance in the region.

- Companies should be aware of the data privacy quirks that exist in Latin America but that are not widespread elsewhere, such as Costa Rica’s “super user” database access for the government, the “right to be forgotten” in Nicaragua, and Mexico’s detailed privacy notice rules but lack of a registration requirement.

- Stay informed. TRUSTe hosted a panel Evolving Privacy Risk in Latin America at the recent Privacy Risk Summit and have featured articles on the blog. Register for the upcoming Privacy Insight Series Webinar on this topic in August.

---

**About TRUSTe**

TRUSTe powers privacy compliance and trust by enabling businesses to use data across their customer, employee and vendor channels. We have nearly 20 years experience and a team of over 150 professionals dedicated to providing data privacy management solutions and services, including assessments, certifications and our SaaS-based Platform. The Data Privacy Management Platform provides control over all phases of privacy; from conducting assessments and implementing compliance controls to managing ongoing monitoring. Companies worldwide rely on TRUSTe to minimize compliance risk and protect their brand. See more at [http://www.truste.com](http://www.truste.com)