Navigating the Gauntlet: A Survey of Data Privacy Laws in Three Key Latin American Countries

John C. Eustice
& Marc Alain Bohn

The Sedona Conference®

Navigating the Gauntlet

A Survey of Data Privacy Laws in Three Key Latin American Countries

By John C. Eustice and Marc Alain Bohn[1]

In October 2000, Argentina enacted Latin America's first comprehensive legislation on personal data protection. Since that time, the region has seen an explosion in laws protecting personally identifiable information, focused primarily on electronic data. While these data protection efforts are, by and large, modeled after similar laws in Europe (in particular, Spain), unlike the European Union ("EU") member states, the laws are not based on a common directive, which has resulted in significant variation in implementation and focus.

At the same time these laws have been enacted, more and more multi-national companies and governments have started using cloud computing and other methods of sharing electronic information across borders, including countries in Latin America. With foreign direct investment in Latin America and the Caribbean topping $173 billion in 2012, the protection of personal data has rapidly become a critical issue for companies operating in the region.[2] Complicating matters, as social networks expand and become more popular in Latin America, more employees are using mobile devices for both business and personal purposes, entwining personal data with business data.

All of these developments challenge traditionally held legal principles of privacy, jurisdiction, and discovery in commercial litigation contexts. This paper examines the laws currently in place in three representative Latin American countries—Argentina, Mexico, and Uruguay—and proposes best practices in alignment with *The Sedona Conference® International Principles on Discovery, Disclosure & Data Protection* ("*Int'l Principles*") for companies, governments, and even individuals involved in litigation in the United States that implicates electronic data originating in each of these three countries. Indeed, the relative dearth of case law or other analyses addressing how U.S. litigation may be impacted by the data privacy and protection laws in place in Argentina, Mexico, and Uruguay highlights the importance of careful application of the practical aspects of the *Int'l Principles*.

These countries are representative of the region in several ways. First, their respective populations vary from small (Uruguay), to medium (Argentina), to large (Mexico). Second, they have varying degrees of commitment to free market principles. Argentina is currently focused on central controls and anti-free market reforms. Mexico and Uruguay seem to be moving in the other direction. Third, these countries present varying levels of corruption risks, with Argentina

---

[1] John C. Eustice is counsel at Miller & Chevalier Chartered, focusing on complex civil litigation faced by foreign and multi-national clients. He is a member of The Sedona Conference® and its Working Group 2. Marc Alain Bohn is a senior associate at Miller & Chevalier whose practice focuses on the Foreign Corrupt Practices Act ("FCPA"), export controls, and economic sanctions. He, too, is a member of The Sedona Conference®.

[2] United Nations Economic Commission for Latin America and the Caribbean ("ECLAC"), *Foreign Direct Investment in Latin America and the Caribbean 2012 Briefing Paper*, at 7 (May 2013).

and Mexico representing higher risk locales and Uruguay on the lower end of the spectrum.[3] Finally, while more than 200 American companies with annual revenues exceeding $10 billion operate in Argentina, Uruguay, and Mexico, these countries demonstrate varying levels of integration with the United States market.[4] Mexico, a member of the North Atlantic Free Trade Agreement ("NAFTA"), has an economy highly entwined with the United States, while the economies of Argentina and Uruguay are more linked to other countries in Latin America and Europe.

Argentina – Leading the Charge

Argentina enacted the *Personal Data Protection Act* ("PDPA") in October 2000.[5] Closely modeled after Spain's *Law on the Protection of Personal Data*, the PDPA provides the regulatory framework for Argentina's data protection regime. Following the PDPA's passage, Argentina issued regulations pursuant to the statute in December 2001.[6] The PDPA, along with these implementing regulations, seeks the comprehensive protection of personal data in Argentina in accordance with the privacy provisions in the country's Constitution, which include a right to privacy and a right to habeas data.[7]

The PDPA, with limited exception, governs the ability of entities and individuals (or "data users") to "process" (i.e., collect, preserve, organize, store, use, evaluate, block, destroy, treat, communicate, or transfer) the "personal data" of others—broadly defined to include any information concerning identified or identifiable individuals or legal entities.[8] Argentina's definitions of "data user" and "processing" are similar to the definitions used by the EU for "data controller" and "processing," respectively.

Additionally, much like the EU, the PDPA affords a higher level of protection to what it terms "sensitive data," which means personal data revealing racial or ethnic origin, political views, religious, philosophical or moral beliefs, union affiliations and any information concerning health status or sexual habits or behavior.[9] No person can be compelled to provide sensitive

---

[3] *See* Transparency International Corruption Perception Index (2012), http://cpi.transparency.org/cpi2012/results/.

[4] *See* Uniworld Business Publications, Inc. (searches conducted 5/7/2013 and 5/28/2013).

[5] *Personal Data Protection Act*, Law No. 25,326 (Oct. 2000).

[6] Decree No. 1.558/2001, Regulations of Law No. 25,326 ("PDPA Regulations").

[7] Arts. 18, 19, 43 of the Constitution of the Argentine Nation (Aug. 22, 1994). Article 43 states as follows: "Any person shall file [a prompt and summary proceeding] to obtain information on the data about himself and their purpose, registered in public records or data bases, or in private ones intended to supply information; and in case of false data or discrimination, this action may be filed to request the suppression, rectification, confidentiality or updating of said data."

[8] Arts. 1-3, PDPA.

[9] Art. 2, PDPA.

data, and it may only be collected and processed in cases of public interest authorized by law or for statistical or scientific purposes, provided that the data owners are no longer identifiable (i.e., rendered anonymous).[10]

The PDPA's jurisdictional scope is less clear than the data privacy laws of other countries. By its terms, however, the PDPA applies to individuals and legal entities, public or private, having a legal domicile or local offices or branches in Argentina, whose data are subject to processing ("data owners").[11] This would appear to include multi-national American companies with offices, subsidiaries, affiliates, or employees operating in Argentina.

Entities and individuals wishing to collect and process personal data in Argentina must, except in limited circumstances, obtain express consent from the data owners in writing or through similar means, depending on the circumstances. To obtain such consent, which, as in the EU, may be revoked at any time, data users must notify data owners in advance and in an express and clear manner of: (1) the purpose for which the personal data will be processed; (2) who the personal data may be provided to; (3) the existence of the relevant database and the identity and location of the person responsible for it; (4) the compulsory or discretionary character of any questions being asked; (5) the consequences of providing the data, of refusing to do so, or of providing inaccurate data; and (6) their right to data access, rectification, and suppression.[12]

As with the Spanish data protection regime, the PDPA also requires all public and private databases to register with Argentina's data protection authority, unless otherwise exempted, before they begin to process personal data.[13] The filing of these registrations is accomplished by submitting a hard copy to Argentina's data protection authority that includes, at a minimum, the following information: (1) the name and address of the data user; (2) characteristics and purpose of the database; (3) nature of the personal data contained in the database; (4) method of collecting and updating the personal data; (5) destination of the personal data and individuals or entities to whom the data may be transferred; (6) manner in which the registered information can be interrelated; (7) means used to ensure data security, including details on the individuals with access to information processing resources; (8) duration for which the data will be stored; and (9) conditions under which third parties can access their personal data, and the procedures to rectify or update such data.[14]

---

[10] Art.7, PDPA.

[11] Art. 2, PDPA.

[12] Arts. 5-6, PDPA. Argentina has not formally decided whether consent obtained from a data owner checking a box on an internet site would be sufficient under these Articles.

[13] Art. 21, PDPA. Exemptions include public databases not created for the purpose of providing reports and private databases created exclusively for personal use. This would not exempt databases created and used by multi-national companies for business communication purposes, which would necessarily include employees' personal data (i.e., identifying information and other personal information).

[14] *Id.*

As Argentina's law was passed in 2000, it understandably does not fully anticipate the current use of cloud or internet-based networks that are physically located outside of Argentina but reach into the country for electronic personal data. For this reason, it is unclear how far Argentina's requirement that data users register all "public and private databases" with its data protection agency actually reaches. While it seems clear that a company setting up a server in Argentina for use by employees working in the country would fall within this requirement, there is no guidance on how the requirement may apply to a cloud system that extends into the country.[15]

In terms of the relationship between data users and data owners, the PDPA identifies a limited number of circumstances in which consent for the processing of personal data is not required, including, among others, situations where the data: (1) are secured from a publicly available source; (2) are collected in connection with the exercise of duties inherent in the powers of the state; (3) are limited to certain basic information, including name, national identity card number, tax or social security identification number, occupation, birth date, address, and telephone number; or (4) arise from a scientific or professional contractual relationship and are necessary for its development or fulfillment.[16]

Unlike in Mexico and certain other Latin American countries, Argentina does not provide an exception to obtaining consent when gathering and producing personal data is necessary in connection with a judicial proceeding. Accordingly, in order to comply with the PDPA, companies involved in U.S. litigation must obtain express, revocable consent from data owners in Argentina before treating processing personal data.

Personal data collected for processing must be: (1) truthful, adequate, pertinent, and proportionate; (2) used only for the limited purpose for which it was legally obtained; (3) collected using fair and honest means; and (4) stored such that data owners can exercise their rights of access. Personal data that is inaccurate or incomplete, in whole or part, must be immediately updated, amended or suppressed. Any personal data collected must be destroyed once the purposes of the collection have been met.[17]

Unlike the data privacy laws of many other countries, the PDPA does not require entities to appoint a personal data officer to oversee compliance and manage requests from data owners.

Personal data can generally only be communicated or transferred with the data owner's prior consent upon being informed of both the purpose of the proposed transfer and the identity of any

---

[15] If the PDPA works similarly to Spain's data protection law, the data user established in Argentina would register its database and identify its cloud services provider (i.e., data processor). In turn, that provider would be subject to the PDPA even if it (and its subcontractors) is actually located outside Argentina.

[16] Art. 5, PDPA.

[17] Art. 4, PDPA.

and all prospective recipients.[18] Where personal data is transferred, the recipient is subject to the same regulatory and legal obligations as the data user.[19]

Cross-border transfers of personal data out of Argentina likewise require the data owner's express consent[20] and may only include countries that provide data protection comparable to the PDPA.[21] Exceptions to this latter requirement include, among others: (1) where the data owner consents to an international transfer without such protection; (2) where adequate protection levels are secured by agreement; and (3) cases of international judicial collaboration or intelligence sharing.[22]

Despite the text of these seemingly onerous regulations, it is not clear how strictly the PDPA prohibitions on cross-border transfers are interpreted or enforced in Argentina. The United States does not have a data protection scheme comparable to the PDPA, which suggests that litigants in U.S. courts would have to obtain the express consent of the data owner for the international transfer of personal data and, if at all possible, secure an agreement with other parties involved in the litigation (or move for an order of court) providing for heightened protection of all personal data culled from Argentine data owners, as called for in the PDPA

Regardless, the PDPA requires the data user to take such technical and organizational measures as are necessary to guarantee the security, integrity and confidentiality of personal data in order to avoid their alteration, loss, or unauthorized access or processing. Such measures must allow the data user to detect any intentional or unintentional distortion or breach of such information.[23] The PDPA does not require data security breaches or losses to be reported to Argentina's data protection authority or to data owners. Pursuant to applicable security regulations, however, all data incidents must be recorded in a security ledger that Argentina's data protection directorate is

---

[18] Art. 11, PDPA. Such consent is not required where, among other reasons: (1) a law so provides; (2) the transfer is made directly between government agencies; or (3) the personal data has been disassociated from the data owner.

[19] *Id.* This would appear to include cloud services providers processing data from Argentina but operating outside Argentina. *See supra*, n.14.

[20] Art. 12, PDPA Regulations. Consent is not required for transfers of personal data from a register that is legally constituted to provide information to the public and which is open to consultation either by: (1) the public in general; or (2) any person who can demonstrate legitimate interest, provided that the legal and regulatory conditions for the particular query are fulfilled.

[21] Art. 12, PDPA.

[22] *Id.* Additional statutory exceptions apply in the following circumstances: (1) the exchange of certain medical data; (2) bank transfers or exchanges; and (3) transfers arranged within the framework of international treaties to which Argentina is a party.

[23] Art. 9, PDPA. The DNPDP provides additional information on its security expectations in resolutions N° 11/2006 and N° 9/2008, which, among other things, detail basic, intermediate, and critical levels of security to be implemented, depending on risk factors such as the nature and sensitivity of the data.

entitled to inspect upon request.[24] This regulation stresses the importance of the fifth of the six *Int'l Principles*—keeping a detailed, accurate log of all efforts to address data protection obligations.

The *Dirección Nacional de Protección de Datos Personales* ("DNPDP") is the national directorate charged with overseeing Argentina's data protection regime. The DNPDP, while characterized as "independent" in the exercise of its duties, is housed within Argentina's Ministry of Justice and Human Rights, from which it receives its operating budget.[25] The DNPDP is responsible for educating parties on the terms of the PDPA, issuing rules and regulations, maintaining the registry of existing databases, monitoring compliance, conducting inspections, and imposing sanctions.[26] To fulfill these responsibilities, the DNPDP has authority to conduct investigations, either upon request of a data owner or data user, or on its own initiative.[27]

Where violations of the law are identified, the DNPDP has the power to impose administrative sanctions, including warnings, suspension, or cancellation of a data user's right to maintain a database, as well as monetary penalties ranging from AR$1,000 to AR$100,000 (approximately $200 to $20,000 USD), depending on the scope and severity of misconduct. Data owners whose rights have been violated may seek a separate recovery for damages arising from the violation of their data protection rights.[28] Beyond monetary sanctions, criminal charges may be brought against violators which carry terms of imprisonment ranging from one month up to three years, depending upon the violator's position of trust and the severity of the violations.[29]

On June 30, 2003, the European Commission formally recognized Argentina as providing an "adequate" level of protection for personal data that comports with the European Union's Directive on the Protection of Personal Data.[30] The European Commission's recognition notwithstanding, critics have questioned Argentina's commitment to enforcing the law. From 2005 to mid-2012, the DNPDP imposed only nineteen sanctions, most of which were in the form of written warnings.[31] Possible explanations for Argentina's failure to adequately enforce the law include insufficient resources and a lack of political will. Indeed, the EU has questioned the

---

[24] Resolution N° 11/2006 and Resolution N° 9/2008.

[25] Resolution N° 1558/01, Art. 29.

[26] Art. 29, PDPA.

[27] Arts. 29, 31-32, PDPA.

[28] Arts. 33-44, PDPA.

[29] Arts. 29, 31-32, PDPA.

[30] Commission of the European Communities, Commission Decision C (2003) 1731 (June 30, 2003).

[31] Enrique M. Stile, *The Current Importance of Implementing Data Protection in Argentina*, Employment Law Alliance (Apr. 10, 2012), http://www.employmentlawalliance.com/firms/marvalar/articles/the-current-importantce-of-implementing-data-protection-in-argentina.

independence of the DNPDP Director because he is both nominated and subject to dismissal by Argentina's Minister of Justice and Human Rights.[32] The EU has also expressed concern about the effectiveness of the DNPDP because it possesses only federal jurisdiction and lacks power when a matter falls within the jurisdiction of an Argentine province.[33]

Despite the apparent lax enforcement of Argentina's data privacy laws, companies operating in Argentina should tread carefully given the scope of the protections outlined in the PDPA. The *Int'l Principles* appear useful in the Argentine context, particularly their focus on transparency, communication, and recordation of an entity's efforts to comply with the law. Specifically, individuals and multi-national companies operating in Argentina and participating in U.S. litigation should consider the following:

- According Due Respect: Both litigants and courts should show respect for the Argentine data privacy law and regulations. With recognition from the European Commission, Argentina's law carries some strict requirements with respect to express consent, registration of databases, and restrictions on international transfers of information. While Argentina's enforcement agency, the DNPDP, does not appear to use its powers as often or as consistently as similar agencies in Europe (or Mexico), data users in Argentina should still make litigants and courts aware of the PDPA and the potential consequences they may suffer for violating it.

- Acting in Good Faith: Given the limits on international transfers of personal data and the need for express consent, data users should bring the PDPA to the attention of the court and litigants at the very beginning of litigation. Indeed, data users should set the table for acting reasonably and in good faith by providing internal policies for obtaining express consent from employees to gather business and personal data, preserving potentially relevant data, and determining whether a database needs to be registered under the PDPA. However, obtaining express consent from other data owners (i.e., clients, individuals, or legal entities) may prove difficult.

- Limiting the Scope of Discovery: With Argentina striving to bring its data privacy and protection laws in line with those in Europe, the *Int'l Principle* counseling a litigant to limit the scope of electronic discovery to only that data relevant and necessary to support a party's claim or defense should be applied as it is in Europe. If identical or substantially similar data may be obtained domestically or from a country with less stringent data privacy laws, such as Brazil,[34] then a data controller should seek to prevent

---

[32] A Journal of Law and Policy for the Information Society 2005–2006, *Argentina's Protection of Personal Data: Initiation and Response*, at 799-800, http://moritzlaw.osu.edu/students/groups/is/files/2012/02/gakh.pdf.

[33] *Id.*

[34] Brazil has no law that specifically addresses data protection. Instead, similar to the United States, Brazil has a patchwork of laws and regulations that extend varying degrees of data protection to particular types of relationships, industry sectors, and professions. *See* Luiz Costa, *A Brief Analysis of Data*

disclosure of data originating in Argentina (at least initially). Whether gathering and producing data via Fed. R. Civ. P. 26(a)(1) or 34, data users should seek to narrow the focus of production through agreement.[35]

- Negotiating a Stipulation / Protective Order: Because of the PDPA's restrictions on cross-border transfers of personal data, parties involved in U.S. litigation should act quickly and invite collaboration with other parties to provide a framework for protecting personal data originating in Argentina in a manner consistent with the PDPA. This process could involve the DNPDP if the data user has questions about the applicability of the PDPA to certain types of data or electronic information systems.[36] Under the PDPA, data users need to ensure via agreement or court order that personal data gathered in Argentina and transferred to the United States is protected in line with the terms of the PDPA and that sensitive personal data is not transferred at all.

- Demonstrating Adequate Process: The PDPA specifically notes that Argentina's data protection directorate is entitled to inspect documents which set forth the steps that the data user has taken to act in good faith and avoid violating the PDPA when gathering, using, and transferring personal data. Accordingly, all data users should ensure careful recordation of all steps taken and considered in order to comply with the PDPA while also meeting their preservation and discovery obligations in U.S. litigation.

- Responsibly Disposing of Protected Data: Data users also must implement policies that facilitate the destruction or return of personal data once the litigation has ended (or the data is no longer necessary or relevant). Ideally, this process should be incorporated into the agreement or court order sought through the fourth *Int'l Principle*.

In sum, Argentina's data privacy and protection regime strives to be as restrictive as those in Europe (and particularly Spain), but falls short in several areas. First, the agency tasked with enforcing the PDPA lacks effective enforcement capabilities compared to European data protection agencies. Second, while the law applies to both individuals and legal entities, the language of the law, drafted in 2000, has not kept pace with technological advancement and therefore remains vague and difficult to apply to cloud or internet-based networks, databases and mobile devices located outside of Argentina. Third, Argentina's law, even if enforced, does not have fines and criminal sanctions on par with those utilized in Europe and other Latin American countries.

Protection Law in Brazil, Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (June 2012).

[35] Data users should also use their judgment to limit the scope of data preservation, acting in good faith and consistent with a reasonable interpretation of what data may be relevant to the case.

[36] One complication with this approach is the possibility that a data user has not registered a database with the DNPDP because the server or system is located outside of Argentina. In this case, the data user should seek counsel and interpretation of the PDPA from an expert in the law.

Mexico – A More Nuanced Approach

Mexico features one of the most recently passed data protection laws in Latin America. Enacted in July 2010, the *Federal Law on the Protection of Personal Data Held by Private Parties* ("LPPD") provides the regulatory framework for data protection by private parties in Mexico.[37] Since passage of the LPPD, Mexico has taken several steps to fully implement the law, including issuing: (a) regulations pursuant to the LPPD which entered into force in December 2011;[38] (b) "Parameters for Self-Regulation" which entered into force in January 2013;[39] and (c) "Privacy Notice Guidelines," which became effective in April 2013.[40]

The LPPD, passed shortly after the 2009 Madrid Resolution outlining International Standards on the Protection of Personal Data and Privacy, seeks to ensure that personal data in Mexico are only processed for legitimate purposes with informed consent, in line with the rights of privacy and self-determination enshrined in Mexico's constitution.[41] In mid-January 2013, the APEC ("Asia-Pacific Economic Cooperation") announced that Mexico had become the second formal participant in the APEC's Cross-Border Privacy Rules ("CBPR") framework, following the United States, which became the first formal participant in July 2012.[42]

The LPPD, with limited exception, governs the ability of private entities and individuals (or "data controllers") to "process" (or access, collect, use, manage, disclose, transfer, or store) the "personal data" of others—broadly defined to include any information concerning an identified or identifiable individual.[43] For instance, personal data include an individual's name, address, telephone number, e-mail address, etc. Additionally, the LPPD affords a higher level of

---

[37] Data protection by public entities in Mexico is governed by the *Federal Law on Transparency and Access to Public Government Information* ("FLTA"), enacted in 2002.

[38] Regulations of the Federal Law on the Protection of Personal Data Held by Private Parties (or "LPPD Regulations") (Dec. 22, 2011).

[39] Parameters for Adequate Application of the Self-Regulatory Scheme Commitments Referred to in Article 44 of the Federal Law for the Protection of Personal Data in Possession of Individuals, Official Gazette of the Federation (Jan. 17, 2013).

[40] Privacy Notice Guidelines (Apr. 17, 2013).

[41] Arts. 6, 7, 16, 20 of the Political Constitution of the United Mexican States. Article 16 amended in June 2009 to include the following language (unofficial translation): "All people have the right to enjoy protection on his personal data, and to access, correct and cancel such data. All people have the right to oppose disclosure of his data, according to the law. The law shall establish exceptions to the criteria that rule the handling of data, due to national security reasons, law and order, public security, public health, or protection of third party's rights."

[42] Cedric Laurant, Mexico Implements APEC's Cross-Border Privacy Rules, Cedric's Privacy Blog, (Feb. 26, 2013), http://blog.cedriclaurant.org/2013/02/26/mexico_implements_apec_cross-border_privacy_rules/.

[43] Arts. 2-3, LPPD.

protection to what it terms "sensitive personal data," which are personal data touching on the most private areas of an individual's life, the misuse of which might lead to discrimination or involve a serious risk.[44] These definitions of "personal data" and "sensitive personal data," while similar to those used by EU countries, include nuances that distinguish Mexico's data privacy law from most other countries' laws.

According to the LPPD Regulations, it applies to personal data: (a) processed by an establishment (i.e., individual, company or subsidiary of a company) of a data controller in Mexico; (b) processed anywhere in the world on behalf of a data controller established in Mexico; (c) where Mexican law is applicable by virtue of a contract or international law; or (d) where the data controller, while not established in Mexico, uses means located in Mexico to process personal data located abroad (which must be more than the mere transit of personal data through Mexico).[45]

Given the language of these Regulations, the LPPD would reach all electronic personal data held by a Mexican subsidiary of a multi-national company, even if the data may be accessed from an office in the United States. Clearly, the Mexican law was drafted with the concept of cloud computing firmly in mind, as it reaches outside of Mexico to data "processed anywhere in the world" on behalf of an entity or individual in Mexico. Under this framework, it appears that a Mexican employee using a mobile device while working in Canada would be creating potentially protectable data.

In instances where private entities or individuals seek to process personal data without violating Mexican law, the LPPD advises adhering to the following eight key principles: (1) Legality: The processing of personal data must adhere to Mexican and international law; (2) Consent: To process personal data, data controllers must generally obtain informed consent from the individuals to whom the data relates (or "data owners"); (3) Notice/Information: Data controllers must issue a privacy notice that communicates to data owners the type of personal data involved and the purposes for which it will be processed; (4) Quality: Personal data that are processed must be pertinent, correct, exact, complete, and up to date; (5) Purpose: Personal data may only be processed for the explicit purposes outlined in the associated privacy notice provided to data owners; (6) Fidelity/Loyalty: Data controllers must protect the interests of the data owners when processing personal data; (7) Proportionality: Data controllers may only process the personal data necessary to fulfill the purposes for which they were obtained; (8) Accountability/Responsibility: Data controllers bear responsibility for the personal data in their custody.[46]

---

[44] Art. 3, LPPD. In particular, this encompasses data related to racial or ethnic origin, current or future health status, genetic information, religion, philosophical or moral beliefs, union membership, political views, or sexual preference. The LPPD also has higher level requirements for data controllers seeking to create databases of "sensitive data." Art. 9, LPPD.

[45] Art. 3, LPPD Regulations.

[46] Art. 6, LPPD; Arts. 10-40, LPPD Regulations.

In accordance with the principles above, companies and individuals wishing to process personal data must, except in limited circumstances, obtain consent from the data owners. To obtain such consent, data controllers must provide data owners with a privacy notice in advance (either electronically, orally, or in writing) that plainly identifies, among other things, the following: the data controller; the personal data at issue and the purpose for which it is being sought; whether the personal data will be transferred; and the data controller's rights, including the right to withhold consent or revoke it prospectively at a later time. Data controllers must also designate a personal data officer to manage requests from data owners seeking to exercise these rights.[47]

For personal data that is neither "sensitive" nor financial in nature, consent may be implied from the lack of any objection by the data owner to the privacy notice (notice and opt out). For financial data, however, consent must be express, and for sensitive personal data, consent must be express *and* written (with notice and an "opt in"). If the purpose for processing the personal data ever changes from the justification originally set out in the privacy notice, consent must be re-obtained.[48]

The LPPD also identifies a limited number of circumstances in which consent for the processing of personal data is not required, including where: (1) a law or resolution from a competent authority so provides; (2) the personal data are publicly available; (3) the personal data is dissociated (i.e., can no longer be used—either by itself or jointly with other information—to identify the individual); (4) the processing of personal data is to comply with the obligations of a legal relationship with the data owner; (5) an emergency exists that could potentially harm an individual or her property; or (6) it is necessary for medical reasons and the data owner is unable to grant consent.[49]

Data controllers may transfer personal data to third parties, either domestically or abroad, if they have obtained consent for such transfers by adequately providing for them in the governing privacy notice. Where personal data is transferred to a third party, the data controller must take sufficient steps to ensure that the third party complies with Mexican law and the applicable privacy notice. The LPPD exempts several types of transfer from the consent requirements, including, among others, transfers: (a) made to a holding company, parent, subsidiary, or affiliate of the data controller; (b) necessary to comply a legal relationship that is with or for the benefit of the data owner; or (c) necessary in connection with a judicial proceeding or are otherwise required by law or authority.[50]

---

[47] Art. 15-18, LPPD; Arts. 22-29, LPPD Regulations. Under the LPPD, data owners enjoy what are known as "ARCO" right, including the right to: (a) access their personal data; (b) rectify erroneous or incomplete personal data; (c) cancel the processing of their personal data; and (d) object to the processing of their personal data. *See* Arts. 16-35, LPPD; Arts. 71-85, LPPD Regulations.

[48] Arts. 8-10, LPPD; Arts. 11-19, LPPD Regulations.

[49] Arts. 10, LPPD.

[50] Arts. 36-37 LPPD; Arts. 60-63, LPPD Regulations.

Given the infancy of the Mexican law, it is not yet clear whether the reference to a "judicial proceeding" in the LPPD means that a data controller in civil litigation in the United States would not need to obtain the consent of a data owner before gathering, processing, and producing his or her personal data in discovery.[51] Not surprisingly, American courts often interpret a foreign law's reference to "judicial proceedings" to include civil litigation in the United States.[52]

The LPPD imposes additional obligations on a data controller once the data has been gathered. Data controllers must establish and maintain adequate physical, technical and administrative security measures designed to protect personal data from unauthorized damage, alteration, loss, or use. Third parties hired to secure personal data on behalf of a data controller assume the obligations as the data controller. Where there has been a breach of personal data, data controllers must promptly notify data owners upon assessing the nature and extent of the breach.[53]

The *Instituto Federal de Acceso a la Información* ("IFAI") is the federal agency that oversees Mexico's data protection regime, with assistance from other agencies, including the Ministry of Economy. IFAI, which has operational, budgetary, and decision-making autonomy, is responsible for, among other things, proactively monitoring and enforcing compliance with the LPPD and LPPD Regulations, responding to complaints from data owners, and imposing sanctions for non-compliance.[54] To fulfill these responsibilities, IFAI has authority to conduct investigations, either upon request of a data owner or data controller or on its own initiative.[55]

Where violations of the law are identified, IFAI can impose monetary penalties from 100 to 320,000 times the daily minimum wage in Mexico City (which amounts to approximately $500

---

[51] Spain's data privacy law includes a similar reference to "judicial proceeding," with the nationality of the proceeding unspecified. In Spain, foreign judicial proceedings are generally included within the definition of the phrase so long as the data controller is the individual or party involved in the proceeding.

[52] For example, in a recent decision in the United States District Court for the Southern District of New York concerning a subpoena served on Banco De La Nacion Argentina ("BNA"), *NML Capital, Ltd. v. Republic of Argentina*, 03 Civ. 8845 (TPG) *et al.*, 2013 U.S. Dist. LEXIS 17572, at *42 (S.D.N.Y. Feb. 8, 2013), the court noted that the text of many countries' data privacy laws "provide no basis for holding that the [consent] exception applies only to a court order from a country's own court." Accordingly, the court found that the laws "do not prohibit BNA from complying with this court's orders to produce responsive documents." *Id.*

[53] Arts. 19-21 LPPD; and Arts. 49-59, LPPD Regulations.

[54] Arts. 38-44, LPPD; and Monika Kuschewsky, *Data Protection & Privacy*, at 357-58 (2012). Earlier this year, a bill was introduced in the Mexican Congress that would amend the Mexican Constitution by, among other things, creating an independent federal agency, separate and apart from IFAI, to protect private sector data. Transitory Art. 5, Proposed Amendments to the Mexican Constitution, at 109 (April 2013). The proposed amendment's ultimate fate is unclear, but it is not expected to pass this year.

[55] Arts. 45-60, LPPD; and Arts. 113-122, LPPD Regulations.

to $1.5 million USD),[56] depending on the scope of misconduct, with fines potentially doubling for repeat offenses. Where the misconduct involves the processing of sensitive personal data, fines can be increased up to double these amounts. Beyond monetary sanctions, criminal charges can be brought against violators carrying terms of imprisonment ranging from three months to five years, depending upon the severity of the violations.[57]

While Mexico's data protection laws are the most recently implemented, they are not as stringent as others in the region (e.g., Argentina and Uruguay) and they have not yet been deemed adequate by the European Union. However, Mexico's data protection regime nevertheless appears well-positioned to be among the most effective in Latin America in terms of protecting personal data. Reasons for this include IFAI's budgetary independence and administrative autonomy, which serve to embolden the agency and leave it free to enforce the law in ways that may be politically unpopular.

IFAI, which is also responsible for overseeing FLTA, the law governing public data protection in Mexico, has not shied away from challenging prominent public institutions in Mexico. Just this year, IFAI has issued prominent directives against the following institutions: Instituto Mexicano del Seguro Social ("IMSS"), the government agency that administers public health, pension and social security programs in Mexico;[58] Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública ("SESNSP"), the government agency for public security;[59] and Petróleos Mexicanos ("PEMEX"), Mexico's state-owned oil company.[60]

IFAI has also exercised its enforcement authority in the private sector, imposing several significant sanctions since the LPPD went into effect. For instance, in December 2012, the IFAI imposed sanctions of over two million Mexican pesos (over $162,000 USD) on Pharma Plus S.A. de C.V., a company which operates pharmacies in Mexico, for failing to provide a sufficient privacy notice to patients whose information regarding filling prescriptions for psychotropic medications was systematically collected.[61]

---

[56] The Council of Representatives of Mexico's National Minimum Wage Commission set the minimum wage for Geographic Area "A," an area which includes Mexico City, at 64.76MXN a day. Cuesta Campos Abogados, *General Minimum Wage 2013* (Jan. 13, 2013), http://www.cuestacampos.com/site/library/general_minimum_wage.html.

[57] Arts. 63-65, LPPD.

[58] Uniradioinforma.com, *Deberá el IMSS información de servicio de traslado colectivo: IFAI* (May 11, 2013), http://www.uniradioinforma.com/noticias/mexico/articulo192248.html.

[59] Cronica.com.mx, *Instruye IFAI informar sobre órdenes de aprehensión pendientes* (May 27, 2013), http://www.cronica.com.mx/notas/2013/756337.html.

[60] Vanguardia, *Ordena IFAI a Pemex estregar copia de contratos* (May 15, 2013), http://www.vanguardia.com.mx/ordenaifaiapemexestregarcopiadecontratos-1741784.html.

[61] Computerworld Mexico, *Farmacias San Pablo, primera compañía multada por violar la LFPDPPP* (Dec. 5, 2012), http://www.computerworldmexico.mx/Articulos/26557.htm.

Though Mexico's data protection law contains nuances distinguishing it from those in Europe and other Latin American countries, the *Int'l Principles* provide a framework for successfully navigating the new law and regulations. Data controllers litigating in the United States should focus on transparency, communication, and reasonable limits on the scope of data collected. Specifically, individuals and multi-national companies operating in Mexico and participating in U.S. litigation should consider the following:

- According Due Respect: Both litigants and courts should show respect for the new Mexican law and regulations. With an independent agency, IFAI, proving willing to enforce Mexico's data privacy and protection schema, data controllers appear to be at risk of fines and even criminal prosecution if they process personal data without consent or misuse any such data.

- Acting in Good Faith: Ultimately, data controllers involved in U.S. litigation will be judged both by a U.S. court and Mexico's IFAI by their reasonableness and good faith. That is why they must identify custodians and categories of potentially relevant protected data as early as possible. Communication between a data controller and the individuals whose data may be relevant to a U.S. legal action is crucial, and should include consent forms and explanations about the need for the data and the individuals' privacy rights. Data controllers have an opportunity in Mexico to obtain "implied consent" of data owners through, for example, a section of an employee handbook. This may be sufficient to allow data controllers to gather, process, and produce employees' personal data that is neither financial nor sensitive in nature (as defined in the Mexican law). Communication between a litigant and adversary is similarly crucial, as a litigant must voice proportionality concerns early to avoid "going down the rabbit hole."

- Limiting the Scope of Discovery: Litigants should attempt to limit the scope of electronic discovery to non-sensitive, non-financial personal data that is relevant and necessary to support a party's claim or defense. If identical or substantially similar data may be obtained domestically or from a country with a less protective data privacy law, then a data controller should seek to prevent disclosure of personal data originating in Mexico (at least initially). Whether gathering and producing data via Fed. R. Civ. P. 26(a)(1) or 34 (or, in certain cases, Fed. R. Civ. P. 45), data controllers should seek to narrow the focus of production through agreement.

- Negotiating a Stipulation / Protective Order: While this concept is certainly not unique to Mexico, parties should act cooperatively when a case involves personal data originating in Mexico. One way to approach this would be to draft a protective order: (a) defining "personal data" in line with Mexico's law; (b) extending special confidentiality protection to any such data produced in the case; (c) defining "sensitive personal data" in line with Mexico's law and excluding such materials from preservation and production or, if such data are relevant and necessary in the case, allowing a party to redact the individuals' names and identifying information so that relevant data may be produced anonymously; (d) seeking an order phasing discovery so that non-personal data may be produced and reviewed before a party processes personal data; and (e) agreeing on a

protocol or legitimization plan that maximizes simultaneous compliance with Mexico's data privacy law and a data controller's preservation and discovery obligations.

- Demonstrating Adequate Process: If a data controller adheres to the first four *Int'l Principles* when dealing with electronic data in Mexico, the fifth should be achievable with one additional step—the data controller should prepare documentation of all efforts taken to comply with Mexico's data privacy law and to comply with its preservation and discovery obligations.

- Responsibly Disposing of Protected Data: The data controller should ensure that it has implemented sufficient policies such that the attorneys and individuals handling protected data are both capable of protecting the data from unwanted disclosure and disposing of the data when no longer necessary.

Overall, Mexico's LPPD provides a clearer, more current construct for protecting personal data, but it is not as restrictive on its face as the laws in place in Argentina or Uruguay. For example, the LPPD allows data controllers to obtain "implied consent" from data owners for transfer of non-sensitive, non-financial personal data. The LPPD also allows more exceptions to consent for transfers to subsidiaries, affiliated companies, and even across borders.

However, data controllers in Mexico should not view the more limited restrictions as an invitation to ignore the LPPD. The law includes substantially larger fines and criminal penalties than Argentina's and Uruguay's law, and the IFAI has demonstrated the autonomy and will to investigate and enforce the LPPD. All of these factors counsel taking the same type of nuanced approach to Mexico's data privacy law that Mexico took in drafting and implementing it.

Uruguay – Leaning Toward Spain

Uruguay enacted the *Protection of Personal Data and Habeas Data Action* ("PDHDA") in August 2008.[62] The PDHDA shares much in common with Argentina's PDPA, as Spain's data protection regime served an influential role in the drafting of both privacy statutes. Since the passage of the PDHDA, Uruguay has issued several directives implementing the statute, the most comprehensive of which came in August 2009.[63]

The PDHDA states at the outset that the right to the protection of personal data "is inherent in the human person," and therefore enshrined in the country's Constitution. Furthermore, according to the PDHDA, the protection of personal data can apply by extension to legal persons, as appropriate.[64]

---

[62] Law No. 18.331 (Aug. 11, 2008).

[63] Decree No. 414/009, Regulations on Law No. 18, 331 (August 31, 2009) ("PDHDA Regulations").

[64] Arts. 1-2, PDHDA. While the Constitution of the Eastern Republic of Uruguay does not expressly acknowledge rights to privacy and the protection of personal data, Article 72 states that "[t]he listing of rights, obligations and guarantees made by the Constitution does not exclude others that are inherent to the human personality or that derive from the republican form of government."

The PDHDA, with limited exception, governs the ability of any person (or "data user") to "process" (or treat, collect, use, form, store, organize, transfer, or communicate) the "personal data" of others—broadly defined to include any information concerning identified or identifiable natural or legal persons.[65]

Additionally, the PDHDA affords a higher level of protection to what it terms "sensitive data," or personal data revealing racial or ethnic origin, political views, religious, philosophical or moral beliefs, union affiliations and any information concerning health status or sexual habits or behavior.[66] No person can be compelled to provide sensitive data, and it may only be collected and treated in cases of public interest authorized by law and for statistical or scientific purposes, provided that the data owners are no longer identifiable.[67]

The processing of personal data is subject to the PDHDA when it is conducted by a data user or processor whose activities are carried out in Uruguayan territory or where the processing is carried out by a means located in the country.[68] Where private entities or individuals seek to process personal data without violating Uruguayan law, they must adhere to seven key principles: (1) legality; (2) truthfulness; (3) purpose/finality; (4) prior informed consent; (5) data security; (6) confidentiality; and (7) responsibility.[69]

Data users who wish to process personal data under the PDHDA must, except in limited circumstances, obtain the express and informed consent of the data owners, which must be freely given and documented.[70] To obtain such consent, which may be revoked at any time, data users must notify data owners in advance of: (1) the purpose for which the personal data will be treated; (2) who the personal data may be provided to; (3) the existence of the relevant database and the identity and location of the person responsible for it; (4) the compulsory or discretionary character of any questions being asked; (5) the consequences of providing the data, of refusing to do so, or of providing inaccurate data; and (6) their right to data access, rectification, and deletion of data.[71] Once the reasons for processing the personal data are no longer present, the personal data must be deleted.

---

[65] Arts. 1-10, PDHDA. Statutory exceptions include databases: (1) held by individuals for personal or household use; (2) used by public safety, defense, state security and law enforcement; (3) created and regulated by special laws.

[66] Art. 3, PDHDA.

[67] Art.18, PDHDA.

[68] Art. 3, PDHDA Regulations.

[69] Art. 5, PDHDA.

[70] Art. 9, PDHDA; Arts. 5-6, PDHDA Regulations.

[71] Arts. 13-17 PDHDA; Arts. 9-16, PDHDA Regulations.

The additional requirement of "informed" consent, which is not expressly mentioned in the Argentine or Mexican laws (even if it may be easily inferred), again makes communication between data users and data owners absolutely crucial. The remaining regulations in this portion of the PDHDA emphasize the need for involving data owner custodians in the data collection process, in addition to providing them with regular updates about the processing and production of any personal data in U.S. litigation.

The PDHDA also identifies a limited number of circumstances in which consent for the processing of personal data is not required, including, among others, situations where the data: (1) are secured from a publicly available source; (2) are collected in connection with the exercise of duties inherent in the powers of the state; (3) are limited to certain basic information, including name, national identity card number, tax or social security identification number, occupation, birth date, address, and telephone number; (4) arise from a scientific or professional contractual relationship and are necessary for its development or fulfillment; or (5) are used for personal or domestic purposes only.[72] This portion of the PDHDA largely mirrors the Argentine PDPA and the Spanish data protection regulations.

Also similar to Argentina's PDPA and the Spanish data protection regulations, Uruguay's PDHDA requires all public and private databases to register with the Uruguay's data protection authority, unless otherwise exempted, before they begin to process personal data.[73] The filing of these registrations is accomplished by submitting a hard copy to Argentina's data protection authority that includes, at a minimum, the following information: (1) the database and the data user; (2) nature of the personal data contained in the database; (3) procedures for obtaining and processing the personal data; (4) means used to ensure data security, including details on the individuals with access to the information treatment process; (5) protection of personal data and the exercise of privacy rights; (6) destination of the personal data and individuals or entities to whom the data may be transferred; (7) duration for which the data will be stored; and (8) conditions under which third parties can access their personal data, and the procedures to rectify or update such data.[74]

Unlike the data privacy laws of many other countries, the PDHDA does not require entities to appoint a personal data officer to oversee compliance and manage requests from data owners.

Personal data can generally only be communicated to another individual or entity: (a) for purposes directly related to the legitimate interests of both the data user and the recipient;[75] and (b) with the data owner's prior consent upon being informed of both the purpose of the proposed

---

[72] Art. 9, PDHDA; Arts. 5-6, PDHDA Regulations.

[73] Arts. 28-29, PDHDA; Arts. 15-16, PDHDA Regulations.

[74] *Id.*

[75] Article 7(f) of the EU Directive features a similar reference to "legitimate interests," which means that the processing of non-sensitive data may be based on a data controller's (or assignee's) legitimate commercial interest when data owners' fundamental rights are not overridden.

transfer and the identity of the prospective recipient.[76] Where personal data is transferred, the recipient is subject to the same regulatory and legal obligations as the data user.[77] It is not yet clear whether the "legitimate interests of both the data user and the recipient" would include disclosure of personal data in the context of civil litigation in the United States. However, it should be noted that litigation could potentially be used as legitimate grounds for processing and producing non-sensitive data, provided that adequate safeguards of data owners' rights are adopted (e.g., through a stipulation or protective order). This concept has been accepted by the Spanish Data Protection Supervisory Authority.

The PDHDA generally prohibits the transfer of personal data to countries or international organizations that do not provide adequate levels of data protection.[78] Exceptions to this prohibition can include, among others, situations in which the transfer is: (1) pursuant to international judicial cooperation or intelligence sharing; (2) related to certain bank transfers or exchanges; (3) allowed under an international treaty to which Uruguay is a party; (4) unambiguously consented to by the data owner; (5) necessary for contractual reasons; or (6) necessary or legally required for the safeguarding of vital interests.[79]

Cross-border transfers of personal data between or within a group of companies is permitted without any additional authorization in situations where the parent, subsidiary, affiliate or branch receiving the personal data has adopted a code of conduct duly registered with the *Unidad Reguladora y de Control de Datos Personales* ("URCDP").[80]

The PDHDA also requires the data user to adopt technical and organizational measures as necessary to ensure the security, integrity and confidentiality of personal data in order to avoid their alteration, loss, unauthorized access, or treatment.[81] Where a data user (or person responsible for processing) detects a security breach that is likely to substantially affect the rights of the data owner or other stakeholders, the data user must inform the persons involved.[82]

The URCDP, a decentralized and autonomous arm of Uruguay's Agency for the Development of Electronic Government and Information Society and Knowledge ("AGESIC"), is the government

---

[76] Art. 17, PDHDA; Art. 14, PDHDA Regulations. Such consent is not required where, among other reasons: (1) it is a law of general interest; (2) the personal data relates to health and sharing it is necessary for reason of public health and safety; or (3) the personal data has been disassociated from the data owner.

[77] *Id.*

[78] Art. 23, PDHDA; Art. 34, PDHDA Regulations.

[79] *Id.*

[80] Art. 35, PDHDA Regulations.

[81] Art. 10, PDHDA; Arts. 7-8, PDHDA Regulations.

[82] *Id.*

authority charged with overseeing the country's data protection regime.[83] The URCDP is responsible for, among other things, advising parties on the terms of the PDHDA, issuing rules and regulations, maintaining the registry of existing databases, monitoring compliance, conducting inspections, and imposing sanctions.[84] To fulfill these responsibilities, the PDHDA provides the URCDP with broad investigative powers, including audit and inspection rights, and subpoena, search and seizure authority.[85]

Where violations of the law are identified, the URCDP may impose administrative sanctions, including warnings, suspension or cancellation of the respective database, and monetary penalties of up to UYU500,000 (approximately $25,000 USD), depending on the scope and severity of misconduct. PDHDA does not provide grounds for criminal enforcement or imprisonment.[86]

On August 21, 2012, the European Commission formally recognized Uruguay as providing an "adequate" level of protection for personal data that comports with the European Union's Directive on the Protection of Personal Data.[87] In addition, on April 10, 2013, Uruguay acceded to Convention 108, the Council of Europe's data standards treaty.[88]

Uruguay's data protection legislation is very similar to Argentina's, though its specific requirements concerning "informed" consent and emphasis on the rights of data owners to maintain access to their personal data counsel full application of those *Int'l Principles* which provide for constant communication between data users and data owners. Individuals and multi-national companies operating in Uruguay and participating in U.S. litigation should consider the following:

- According Due Respect: Both litigants and courts should show respect for the Uruguay law and regulations, which has been judged adequate by the European Commission. Uruguay's push to accede to Convention 108 also bolsters the credibility of the PDHDA. While Uruguay's data protection agency, the URCDP, does not have a long history of enforcing the PDHDA or imposing fines and penalties, Uruguay's recent push for full European recognition may portend robust enforcement efforts in the future.

- Acting in Good Faith: The need for data users to act reasonably and in good faith, particularly with respect to communicating with and obtaining express consent from data

---

[83] Arts. 31-36, PDHDA Regulations.

[84] *Id.*

[85] *Id.*

[86] Art. 35, PDHDA.

[87] Commission of the European Communities, Commission Decision C (2012) 5704 (Aug. 21, 2012).

[88] Stanislava Gaydazhieva, *Uruguay Joins European Data Protection Convention*, New Europe Online, (Apr. 12, 2013), http://www.neurope.eu/article/uruguay-joins-european-data-protection-convention.

owners, is emphasized in the PDHDA. Entities operating in Uruguay need to implement and adhere to policies that both educate data owners and provide a framework for obtaining their informed consent when data users need to preserve potentially relevant data and determine whether a database needs to be registered under the PDHDA.

- Limiting the Scope of Discovery: Even more important than in Mexico or Argentina, companies operating in Uruguay and litigating in the United States need to limit the scope of discovery into the personal data of data owners located in Uruguay. Given that data users must obtain the informed consent of data owners, and because that consent may be revoked at any time for any reason, data users continually risk violating the PDHDA when processing and producing personal data. Accordingly, parties should hew closely to this *Int'l Principle*, which counsels working with opposing parties and the court to limit the scope of electronic discovery to only that data relevant and necessary to support a party's claim or defense.

- Negotiating a Stipulation / Protective Order: The PDHDA's restrictions on transfers to countries with lesser levels of data protection, which includes the United States, means that a data user in Uruguay involved in U.S. litigation should proactively seek a stipulation or protective order providing confidentiality and other safeguards for any personal data gathered, processed, and potentially produced in the case. Under the PDHDA, in order to transfer personal data from Uruguay to the U.S. in a civil litigation context, it appears that a data user must provide comparable safeguards as discussed above or obtain the unambiguous (and revocable) consent of each data owner.

- Demonstrating Adequate Process: As in Argentina, Uruguay's data privacy law empowers its data agency to monitor compliance with the law. Accordingly, all data users should keep track of steps taken and considered in order to comply with the PDHDA while meeting their preservation and discovery obligations in U.S. litigation.

- Responsibly Disposing of Protected Data: As in both Argentina and Mexico, data users in Uruguay must implement policies that require the disposal of personal data as soon as practicable. Once again, this process would be best incorporated into the agreement or court order sought through the fourth *Int'l Principle*.

Uruguay's data protection structure has the potential to become the most restrictive in Latin America, provided the URCDP diligently enforces the PDHDA. The URCDP does not appear to suffer from the criticized lack of effective autonomy of the DNPDP in Argentina, but it does lack the history of enforcement demonstrated by Mexico's IFAI. Only time will tell whether Uruguay will implement and enforce its European-style data privacy and protection laws.

The data protection regimes currently in place in these three representative Latin American countries share a great deal in common, as evidenced by our survey. However, the variation that does exist, particularly in key areas such as cross-border transfers and actual enforcement of the statutes, represents a significant challenge for companies seeking to do business across Latin American borders.