Bloomberg BNA

Privacy and Security Law Report®

Privacy in Latin America and the Caribbean

By Cynthia Rich

Introduction/Region At-a-Glance

Thirteen jurisdictions in Latin America now have comprehensive privacy laws including: Argentina, Aruba, Bahamas, Chile, Colombia, Costa Rica, Curacao, Dominican Republic, Mexico, Nicaragua, Peru, Trinidad and Tobago[1] and Uruguay.[2] The two laws that are most closely aligned with the European laws (and thus deemed to the European Commission to provide adequate protection) are Argentina and Uruguay.

Other countries such as Brazil, Ecuador and territories such as the Cayman Islands have draft bills that have either been or are expected to be introduced to their legislatures. In addition, Chile, which has had a high-level data protection law since 1999, may amend its existing law in 2015 to include registration, impose cross-border restrictions and establish a data protection regulator.

[1] On Jan. 6, 2012, Trinidad and Tobago adopted a Data Protection Act, 2011; currently, the only provisions in force pertain to the establishment of the data protection authority. The Data Protection Act is available at http://www.ttparliament.org/legislations/a2011-13.pdf.

[2] Saint Lucia adopted legislation in 2011, but the law has not yet gone into effect.

Cynthia Rich is a senior advisor at the Washington office of Morrison & Foerster LLP. As a member of the firm's international Privacy and Data Security Practice since 2001, Rich works with clients on legal issues relating to privacy around the world.

This article examines the commonalities and differences among the privacy laws in the region and discusses current trends and new developments.

Common Elements Found In Latin American Laws

Notice: All of the laws in Latin America include some type of notice obligation. That is, every law requires that individuals be told what personal information is collected, why it is collected and with whom it is shared.

Choice: Every privacy law also includes some kind of choice element. The level or type of consent varies significantly from country to country. For example, Colombia has a much stronger emphasis on affirmative opt-in consent than does Mexico, but all of the laws include choice as a crucial element in the law.

Security: Furthermore, all of the laws require organizations that collect, use and disclose personal information to take reasonable precautions to protect that information from loss, misuse and unauthorized access, disclosure, alteration and destruction. Some of the countries, such as Argentina and Mexico, have specified in greater detail how these obligations are to be met.

Access and Correction: One of the core elements of every privacy law is the right of all individuals to access the information that organizations have collected about them and, where possible and appropriate, correct, update or suppress that information. Interestingly, compared to their European and Asian counterparts, most countries in Latin America require organizations to respond to access and correction requests in a much shorter period of time.

Data Integrity: Organizations that collect personal information must also ensure that their records are accurate, complete and kept up-to-date for the purposes for which the information will be used.

Data retention: Generally, these laws require organizations to retain the personal information only for the period of time required to achieve the purpose of the processing. Some laws may mandate specific retention periods, while others set limits on how long data may be retained by an organization once the purpose of use has been achieved.

Differences in Approaches

While the core data protection principles and requirements are embodied in all of these laws, specific requirements, particularly with respect to cross-border

 ISSN 1538-3423

transfers, registration, data security, data breach notification and the appointment of a data protection officer (DPO) vary widely from each other and from laws in other regions of the world.

For example, more than two thirds of the countries in this region restrict cross-border transfers of personal information to countries that do not provide adequate protection. However, unlike the European approach (and more like the approach in countries such as South Korea or Singapore), there is a heavy reliance on consent to legitimize transfers to inadequate countries. Some permit the use of contracts or internal rules in lieu of consent, and some require both. In almost all cases, the data protection authorities (DPAs) have not specified what must be contained in these contracts or rules. Most of the Latin American laws do permit companies to transfer data to another country if it is a contractual necessity. But transfers in most countries cannot be legitimized based on the legitimate interests of the company (unlike in many European countries). From a practical point of view, most of the DPAs in the region have not issued lists of countries that they believe provide adequate protection, thus, companies are left to assume that all countries are deemed to be inadequate and must put in mechanisms (such as consent or contracts) to satisfy the rules.

The differences widen when comparing their respective rules on registration, data breach notification, security and DPO obligations: Almost half of the countries require registration; more than one third require notification in the event of a data breach; and about one quarter require the appointment of a DPO. In addition, almost two thirds of the laws in the region require that access and/or correction requests be responded to within 10 days (an exceedingly short time frame), and almost one quarter protect personal information of both natural and legal persons.

Lastly, two of the countries, Nicaragua and Costa Rica, have unusual provisions. In Costa Rica, organizations that register databases with the DPA must provide the regulator with an access profile so that the DPA may access and consult the database, at any time and without restriction. In Nicaragua, the law provides for the right to be forgotten, a provision that is beginning to pop up with greater frequency in privacy litigation and proposed legislation.

A careful read of these laws is imperative, therefore. These differences pose challenges to organizations with respect to the adjustments that may be required to global and/or local privacy compliance practices as well as privacy staffing requirements. Compliance programs that comply with only European Union and Asian obligations will run afoul of many of the Latin American and Caribbean country obligations.

A country-by-country summary of the obligations in these key areas is provided below. Other noteworthy characteristics are also highlighted and, where applicable, the responsible enforcement authority is identified. In addition, a chart is provided at the end to show at a glance the countries with mandatory cross-border, DPO, data security breach notification and registration obligations.

Trends

Enforcement

Violations of these laws can result in significant criminal and civil and/or administrative penalties being imposed; however, the level of enforcement by the authorities within the region has been relatively low, in part because it has taken time for some of the authorities to establish themselves. Of all of the authorities in the region, the DPA in Mexico has been the most active in issuing fines, some of which have been quite high. For example, in the past couple of years the Mexican DPA imposed a 16.2 million Mexican peso ($1 million) fine on Banamex, Mexico's second largest bank, for privacy law violations pertaining to individuals' deletion and opposition rights (12 PVLR 1038, 6/17/13). It also fined Telcel, a cellular company, 10 million Mexican pesos ($651,370) for the misuse of frequent contact phone numbers of a client to collect a debt for mobile service (12 PVLR 1912, 11/11/13), and it fined Tarjetas Banamex 9.9 million Mexican pesos ($644,857) for the failure to provide correction and deletion rights. Recently, the Mexican DPA warned Google Inc. that it could face a fine up to 22.4 million Mexican pesos ($1.4 million) for failing to delete personal information from its search engine (14 PVLR 259, 2/9/15).

The level of enforcement by the authorities within Latin America and the Caribbean has been relatively low, in part because it has taken time for some of the authorities to establish themselves.

Many of these fines are in the process of being contested by the companies; however, in November 2014, the Mexican DPA announced that, for the first time, an unnamed company had voluntarily agreed to pay a fine of 129,000 Mexican pesos ($8,403) for breaching the law. The violation was for failing to give a privacy notice to one of its employees about the purposes for which it was collecting and using the employee's personal information.

Moreover, in what could be a growing trend in the country, Mexico's consumer protection agency, Profeco, is using its authority under the country's Consumer Protection Law to sanction electronic commerce companies for unfair practices, including those that violate consumers' privacy rights. In September 2014, the agency imposed a 3.5 million Mexican peso ($227,980) fine on e-commerce retailers after it conducted on its own initiative an inspection of online stores in order to verify their compliance with e-commerce, online consumer protection, electronic contracting and privacy regulations. The agency determined that the stores' online terms and conditions and privacy notices were ambiguous and that they failed to disclose mandatory information that must be provided to consumers before a transaction takes place and breaches consumers' privacy rights.

DPAs in Colombia and Peru are also starting to become more active, and there have been recent cases in which they have imposed large fines for privacy violations. For example, the Peruvian DPA issued its first enforcement sanction in October 2014. It fined the Peruvian company DATOSPERU.ORG approximately $78,600 for publishing sensitive personal information of two citizens on it Web page without their consent. In

  PVLR ISSN 1538-3423

Colombia, the DPA fined Redcord, an umbilical cord stem cell bank, $50,000 for privacy law violations involving the use of sensitive personal information for marketing purposes without the individual's consent. The fine was the highest fine issued to date by the Colombian DPA.

Other than Mexico, Columbia and Peru, the other country in the region that actively protects privacy rights is Brazil, despite the fact that it does not yet have in place a comprehensive privacy law.

The other country in the region that actively protects privacy rights is Brazil, despite the fact that it does not yet have in place a comprehensive privacy law. Private lawsuits and government enforcement actions are actively pursued whenever an individual's rights to privacy, as provided for under the Constitution, Civil Code, Consumer Protection Law and the recently enacted Internet Bill of Rights (Internet Law), are perceived to have been violated. In particular, the enactment of the Internet Law in April 2014 has sparked enforcement actions by the Consumer Protection Agency and the Public Attorney's Offices at the federal and state levels. The Internet Law prohibits Internet service providers, search engines, social media websites and online retailers who collect personal information from Brazilian consumers from sharing personal information as well as connection and application access logs with third parties, except with the user's express consent.[3] In addition, there is a provision that allows the government to enforce against offshore businesses that collect, maintain or store data from Brazilian users.

In 2014, the Consumer Protection Agency fined the Brazilian telecommunications company Oi SA 3.5 million Brazilian reals ($1.2 million) for recording and selling subscriber browser data (13 PVLR 1343, 8/4/14). Oi partnered with a U.K.-based online advertising company Phorm to develop profiles of users' browsing practices, which were then sold to online advertising firms to generate customized advertisements.

There have also been actions by the Brazilian Public Attorney's Offices at the federal and state levels brought against large companies such as Apple Inc., Google and Microsoft Corp. The Federal Public Attorney's Office brought suit to force Google to provide application logs and personal information of users through its local subsidiaries for criminal investigation purposes. A state Public Attorney's Office also filed a civil action against these three companies to stop the distribution of an anonymous social networking application (app) that permits customers to post anonymous messages. The action was taken after users complained that they were harmed by rumors spread via the app.

Privacy Legislation Under Development

More laws are expected to be enacted, possibly sometime during 2015. Late in 2014, the government of Chile held a public consultation on proposed legislation and published its responses to questions received from the general public, industry and other organizations during the consultation. The proposed legislation, if adopted, would, among other things, create a DPA, require registration of databases and impose restrictions on cross-border transfers. A bill is expected to be submitted to the legislature this year.

Brazil is also working on draft privacy legislation. In January 2015, the Brazilian Ministry of Justice launched a public consultation on a new draft privacy law that, if adopted, would apply to the processing of personal information by public and private sector organizations, regardless of the country in which the organizations are headquartered and the country in which the databases are located, provided that the processing is carried out in Brazil or the personal information is collected within Brazil (e.g., the individual is located in Brazil at the time the data are collected). The proposed scope of the law appears to cover outsourced data processing in Brazil and, as a result, may impose a complex and burdensome set of rules on such activities.[4]

Moreover, the proposed law would restrict cross-border transfers to countries that do not provide similar protection unless one of the limited exceptions applied or the individual specifically consented to the transfer after being given information on the international character of the operation and the risks involved in the transfer, based on the vulnerabilities specific to the destination country. The regulator would identify which countries do not provide similar protection. The draft law also would require the appointment of a DPO and the regulator to be notified about data breaches. Individuals would have to be given immediate notice of a data breach involving their personal information in cases where the incident jeopardized their personal safety or could cause them damage.

Like Chile and Brazil, the Cayman Islands recently conducted a public consultation on draft privacy legislation.[5] The proposed law would establish a DPO, require registration and data breach notification and restrict cross-border transfers. Lastly, it appears that Ecuador is also contemplating privacy legislation, but the text of that law has not yet been made public.

Country-by-Country Review of Differences

ARGENTINA

The Personal Data Protection Act (Argentine Law), enacted in 2000, protects all personal information of natural persons (living and deceased) and legal entities recorded in public or private data files, registers and data banks, established for the purpose of providing reports.[6] Argentina was the first country, and currently only one of two countries in Latin America, to be recog-

[3] The Internet Law is available, in Portuguese, at http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm.

[4] Further information about the consultation on the Preliminary Draft Bill for the Protection of Personal Data, including the text of the bill, is available, in Portuguese, at http://participacao.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/.

[5] The Cayman Islands draft legislation is available at http://bit.ly/1QphjVj.

[6] The Argentine Law is available, in English, at http://mofoprivacy.blob.core.windows.net/privacylibraryfiles/Argentina-DataProtectionAct.pdf. It is available in Spanish at

nized by the European Union as providing an adequate level of protection for personal information transferred from the EU/European Economic Area (2 PVLR 737, 7/7/03).

In Brief. *The Argentine Law restricts cross-border transfers to countries that do not provide adequate protection, requires registration and imposes detailed security requirements. However, there is no obligation to give notice in the event of a data security breach or appoint a DPO.*

Special Characteristics

Data Protection Authority. The National Directorate for Personal Data Protection, located within the Justice and Human Rights Ministry, is responsible for enforcement of the Argentine Law.[7]

Cross-Border Transfers. The transfer of personal information to countries outside Argentina that do not provide an adequate level of data protection is prohibited, unless the individual has provided his/her express consent to the transfer or another exception applies. However, the DPA has not officially recognized any jurisdiction as having an adequate or inadequate level of data protection.

Consent is not required to transfer to a service provider in an inadequate country, provided that there is an appropriate contract in place. The DPA has approved specific clauses for certain contracts, but it has done so on a case-by-case basis. Until recently, there were no models issued by the DPA. Now, however, the DPA has made available text clauses that it will use as a parameter for assessing international transfer agreements.

Data Security. After the Argentine Law was enacted, regulations imposing additional security requirements were issued. The security measures are divided into three levels: Basic or Low level measures for all databases containing personal information; Medium level measures for private companies acting as public utilities or public companies, and the owner of the database is bound by a duty of secrecy imposed by law (e.g., bank secrecy); and High level or critical level measures for all databases containing sensitive personal information.[8]

Registration. Organizations must register their databases with the DPA. The registration covers the processing of all personal information for all purposes.

ARUBA

The Personal Data Protection Ordinance (Aruba Law), enacted in 2011, establishes rules for the protection of privacy in connection with the collection and disclosure of personal information of natural persons by both the public and private sectors.[9] The Aruba Law applies to all files of data controllers established in Aruba, regardless of where such files are located (in or outside Aruba), provided that the files contain personal information of individuals settled in Aruba.

In Brief. *The Aruba Law imposes restrictions on cross-border transfers but does not require database registration, the appointment of a DPO or data security breach notification.*

Special Characteristics

Data Protection Authority. The Minister of Justice is responsible for enforcement of the law.[10]

Cross-Border Transfers. The Aruba Law prohibits transfers of personal information into the files to which the law is not applicable, to the extent that the Minister has declared that such transfers would result in a serious disadvantage for individuals' privacy. The Minister can issue a waiver for files located outside Aruba if the law of the country in which the file is located provides an equivalent level of privacy and data protection.

BAHAMAS

The Data Protection (Privacy of Personal Information) Act 2003 (Bahamas Law) protects the personal information of natural persons and applies to processing of such data by both the public and private sectors.[11]

In Brief. *The Bahamas Law does not require database registration, impose mandatory DPO and data security breach obligations or restrict cross-border transfers. However, with respect to the latter three areas, the DPA has issued nonbinding guidance. In addition, the Bahamas Law is unusual because there are no explicit notice and consent requirements.*

Special Characteristics

Data Protection Authority. The Office of the Data Protection Commissioner is responsible for investigating any contraventions of the Bahamas Law, either of its own volition or as a result of a complaint by an individual concerned.[12]

Notice and Consent. While there are no explicit notice and consent requirements set forth in the Bahamas Law, the DPA interprets the obligation to collect and process personal information fairly to mean that individuals must be made aware of certain information regarding the processing of their personal information and must consent to that processing, or one of the other conditions specified in the Bahamas Law must apply.

Cross-Border Transfers. The DPA has the authority to prohibit the transfer of information outside the Bahamas where there is a failure to provide protection either by contract or otherwise equivalent to that provided under the Bahamas Law. The DPA has issued nonbinding guidance listing the conditions, similar to those found in EU laws, which need to be met to transfer personal information cross-border.

---

http://www.infoleg.gov.ar/infolegInternet/anexos/60000-64999/64790/norma.htm.

[7] The website address for the Argentine DPA is http://www.jus.gob.ar/datos-personales.aspx.

[8] *See* Disposition 11/2006 (Security Measures), Sep. 20, 2006, available, in English (unofficial translation), at http://bit.ly/1DZQr7M and, in Spanish, at http://www.jus.gob.ar/media/33445/disp_2006_11.pdf.

[9] The Aruba Law is available, in Dutch, at http://bit.ly/1GDJoFp.

[10] The website address for the Aruba Ministry of Justice is http://www.overheid.aw/governance-administration/ministry-of-justice_3989/.

[11] The Bahamas Law is available at http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0003/DataProtectionPrivacyofPersonalInformationAct_1.pdf.

[12] The website of the Bahamas DPA is at http://bit.ly/1DK5HWs.

  PVLR ISSN 1538-3423

Data Protection Officer. There is no obligation under the Bahamas Law to appoint a DPO; however, the DPA recommends it.

Data Security Breach Notification. There is no obligation on organizations to give notice in the event of a data security breach; however, there is voluntary DPA Guidance on Managing a Data Security Breach.[13] The guidance states that organizations may choose to provide notice in the event of a breach of security resulting in unauthorized access to; alteration, disclosure or destruction; or accidental loss or destruction of personal information.

CHILE

Law No. 19.628 of Protection of Personal Data (Chilean Law), the first privacy law enacted in Latin America in 1999, regulates the processing of personal information of natural persons by both the public and private sectors.[14]

In Brief. *The Chilean Law does not restrict cross-border transfers or impose data security breach notification, DPO or registration requirements. Unlike most privacy laws, the Chilean Law does not establish a DPA to oversee enforcement; civil courts are responsible for enforcing the law.*

COLOMBIA

Enacted in October 2012, Law No. 1581 ''Introducing General Provisions for Personal Data Protection'' (Colombian Law) sets forth general rules for the protection of personal information of natural persons by both the public and private sectors, including special protections for children.[15] The Colombian Law is intended to complement a law enacted in 2008 that applies to personal credit information only. Organizations had six months (until April 17, 2013) to come into compliance with the Colombian Law.

In Brief. *The Colombian Law imposes DPO, data security breach notification and registration requirements and restricts cross-border transfers to countries that do not provide adequate protection. In addition, some additional data security measures are required.*

Special Characteristics

Data Protection Authority. The Personal Data Protection Division, the organization within the Superintendence of Industry and Commerce responsible for performing the functions of the DPA, is authorized to carry out investigations on the basis of complaints or on its own initiative.[16]

Cross-Border Transfers. The transfer of personal information to countries outside Colombia that do not provide an adequate level of data protection is prohibited, unless the individual has provided his/her express consent to the transfer, the transfer is necessary to execute a contract between the individual and the organization or another exception applies. The DPA may approve transfers to nonadequate countries that do not fall under one of the above-listed exceptions by issuing a conformity declaration (declaración de conformidad). The additional requirements and obligations that must be satisfied before the DPA may issue such declarations are expected to be addressed in the forthcoming implementing regulations.

Once the National Registry of Databases is established, organizations and service providers that carry out processing of personal information in Colombia must register with the DPA.

Data Protection Officer. Every organization and service provider must appoint a person or department responsible for protecting personal information and processing requests from individuals who seek to exercise their rights under the law.

Data Security. The DPA is required to issue instructions related to the security measures for processing personal information. If an organization breaches its duties and obligations under the law and the DPA has to decide whether or not to impose penalties, it will take into account the extent to which the organization has in place the proper security policies and measures for the proper handling of the personal information.

Data Security Breach Notification. Both the organization and the service provider must inform the DPA about any violations of security codes and any risks in the administration of information of individuals. There is no obligation to give notice of such breaches directly to individuals.

Registration. Once the National Registry of Databases is established, organizations and service providers that carry out processing of personal information in Colombia must register with the DPA. A record will be entered into the National Registry of Databases, which will be available for public consultation. It is quite unusual to require service providers to file registrations with the DPA. The government is expected to issue the regulations establishing the National Registry in April 2015.

COSTA RICA

Law No. 8968 on the Protection of the Person Concerning the Treatment of Personal Data (Costa Rican Law) came into force Sept. 5, 2011.[17] It applies to automatic and manual processing of personal information of natural persons by both public and private entities. Companies had until March 5, 2013 to bring their practices into compliance with the Costa Rican Law.

In Brief. *The Costa Rican Law requires data security breach notification and registration. It also imposes special data security and ''Super User'' obligations but*

[13] The Guidance on Managing a Data Security Breach is available at http://bit.ly/1Gc8kP6.

[14] The Chilean Law is available, in Spanish, at http://www.leychile.cl/Navegar?idNorma=141599&buscar=19628.

[15] The Colombian Law is available, in Spanish, at http://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/LEY-1581-DEL-17-DE-OCTUBRE-DE-2012.pdf (11 PVLR 1573, 10/29/12).

[16] The website address for the Colombian DPA is http://www.sic.gov.co/drupal.

[17] The Costa Rican Law is available, in Spanish, at http://www.tse.go.cr/pdf/normativa/leydeprotecciondelapersona.pdf.

does not require the appointment of a DPO or restrict cross-border transfers. However, there are general rules that apply to all data transfers.

Special Characteristics

Data Protection Authority. Prodhab, established in March 2012, is responsible for creating a database registry, ensuring compliance with the Costa Rican Law and issuing implementing regulations.[18]

Cross-Border Transfers. There are no limitations on cross-border transfers; however, the general rules for any transfer of databases and/or personal information apply. In particular, express written consent (or a contract) is required to share or transfer personal information. The Costa Rican Law does not include any other legal bases for transferring data, and this rule applies broadly to all transfers without explicit indication of whether the transfer occurs within or outside Costa Rica.

Data Security. In addition to the basic security obligations, the Costa Rican Law requires organizations to issue a ''Performance Protocol'' that will regulate all the measures and rules to be followed in the collection, management and handling of the personal information. In order to be considered valid, the Performance Protocol (and any subsequent amendments) must be registered with the DPA.

Data Security Breach Notification. Organizations must inform individuals about any irregularities in the processing or storage of their personal information, or when the organization becomes aware of such irregularities. Irregularities include but are not limited to loss, destruction and/or misuse that result from a security vulnerability or breach. They must inform individuals within five working days from the time the vulnerability occurs so the individuals may take appropriate action.

Registration. Every database that is established for distribution, promotion or commercialization purposes must be registered with the DPA.[19] According to a FAQ posted on the DPA website, human resources databases that are used for the exclusive use of the company do not need to be registered.[20]

'Super User.' The Costa Rican Law has a very unusual requirement not found in any other privacy law worldwide. Organizations that registered databases with the DPA must provide the regulator with an access profile so that the DPA may access and consult the database, at any time and without restriction. In FAQs issued by the DPA on its website,[21] the DPA states that it will only access databases in response to a complaint or when there is evidence of possible law violations. It further states that the ''Super User'' provision should not be interpreted as providing the DPA with absolute power to access all information contained in these databases. In particular, the DPA does not have the ability to access databases containing information on banking transactions, suppliers and corporate financial statements.

[18] The website address for the Costa Rican DPA is http://prodhab.go.cr.

[19] The registration form is available, in Spanish, at http://prodhab.go.cr//tramites/?inscripcion-de-bases-de-datos.

[20] *See* FAQ 6, in Spanish, at http://prodhab.go.cr//preguntas-frecuentes/?empresas.

[21] *See* FAQ 11, in Spanish, at http://prodhab.go.cr//preguntas-frecuentes/?empresas.

CURACAO

The Personal Data Protection Act (Curacao Law), which took effect Oct. 1, 2013, regulates the processing of personal information of natural persons by both the public and private sectors.[22] The Curacao Law is modeled on the Dutch Data Protection Law.

In Brief. *The Curacao Law restricts the cross-border transfer of personal information to countries that do not provide adequate protection. However, there are no DPO, data security breach notification and registration requirements. There is also no required time frame specified for responding to access or correction requests.*

Special Characteristics

Data Protection Authority. The College Bescherming Persoonsgegevens supervises compliance with the Curacao Law.[23]

Cross-Border Transfers. Personal information may only be transferred to a country outside the Kingdom of the Netherlands [24] if that country ensures an adequate level of protection. Where there is no adequate level of protection, the data transfer may take place provided that:

- the individual has provided his/her explicit consent;
- the transfer is necessary for the performance of a contract between the individual and the data controller or for actions to be carried out at the request of the individuals and which are necessary for the conclusion of a contract;
- the transfer is necessary for the conclusion or performance of a contract concluded or to be concluded between the data controllers and third parties in the interests of the individuals;
- the transfer is necessary on account of an important public interest, or for the establishment, exercise or defense in law of any right;
- the transfer is necessary to protect the vital interests of individuals;
- the transfer is carried out from a public register set up by law or from a register that can be consulted by anyone or by any persons who can invoke a legitimate interest, provided that in the case concerned the legal requirements for consultation are met; and
- the transfer has been approved by the DPA.

DOMINICAN REPUBLIC

The Organic Law 172-13 on the Protection of Personal Data (Dominican Law), which took effect Dec. 13,

[22] The Curacao Law is available, in Dutch, at http://mofoprivacy.blob.core.windows.net/privacylibraryfiles/Curacao-PRIVACY-ACT.pdf.

[23] The website address for the Curacao DPA is not available.

[24] [Editor's note: The Kingdom of the Netherlands consists of the Netherlands, Aruba, Curacao and Sint Maarten.]

  PVLR ISSN 1538-3423

2013, is the most recent law enacted in the region.[25] The Dominican Law protects personal information filed in public or private archives, public records and data banks intended to provide reports. The Dominican Law also regulates credit information companies, the provision of credit reference services and the supply of information on the market to ensure respect for privacy and the rights of the information owners.

The Dominican Law is the most recent law enacted in the region.

In Brief. *In contrast to the cross-border rules found in other countries in the region, the Dominican Law imposes a common set of legal bases for all international transfers, regardless of their destination. Registration/supervision requirements apply only to public or private data banks that are intended to provide credit reports. Such data banks are subject to the inspection and supervision of the Superintendence of Banks. There is also no obligation to appoint a DPO or to notify individuals or the regulator in the event of a data security breach. The Dominican Law does not establish a DPA to oversee compliance; however, the Superintendence of Banks is the entity authorized to regulate credit information companies.*

Special Characteristics

Cross-Border Transfers. Personal information may only be transferred internationally in certain circumstances such as:

- the individual consents to authorize the transfer of information or when the laws so allow;
- the transfer is necessary for the execution of a contract between the individual and the organization, or for the execution of pre-contractual measures;
- the transfer concerns bank or security transfers with regard to the respective transactions and in accordance with the applicable legislation;
- the transfer has been agreed or considered in the framework of international treaties or conventions, or in free-trade treaties of which the Dominican Republic is a part; or
- the transfer of legally required information is to safeguard public interest or for the acknowledgement, exercise or defense of a right in a judicial process, or is required by a tax or customs administration to fulfill its duties.

MEXICO

The Federal Law on Protection of Personal Data Held by Private Parties (Mexican Law), enacted in 2010, regulates the processing of personal information of natural persons by private sector organizations but does not apply to duly licensed credit reporting companies.[26]

In Brief. *The data protection rules in the Mexican Law have a number of important differences from those found elsewhere in the region. For example, the notice and data security obligations are subject to detailed rules. Unlike many laws in the region, the Mexican Law does not require registration, but it does require the appointment of a DPO and data security breach notification. In addition, domestic and international transfers are largely subject to the same requirements.*

Special Characteristics

Data Protection Authority. The Federal Institute for Access to Information and Data Protection (IFAI) is responsible for disseminating information on data protection and compliance with the Mexican Law.[27]

Notice. In 2013, the DPA issued Guidelines that provide for three different types of privacy notices: comprehensive, simplified and short.[28] A comprehensive privacy notice must always be made available; however, depending on the circumstances of the data collection, a simplified or short privacy notice may be provided first. The Guidelines state expressly that provision of a simplified or short privacy notice does not relieve the organization of its obligation to make available a comprehensive privacy notice.

Simplified or Short Privacy Notice. Where personal information is obtained directly from the individual by any electronic, optical, audio or visual means, or through any other technology, the organization must immediately provide the individual with at least the information regarding the identity and domicile of the organization and the purposes of the data processing, as well as provide the mechanisms for the individual to obtain the full text of the privacy notice. Where cookies, Web beacons or similar technologies are used, a communication or warning must be placed in a conspicuous place to inform the individual about the use of these technologies and how the technologies can be disabled by the individual.

Data Protection Officer or Office. The Mexican Law requires any entity that collects personal information to appoint a DPO or office to promote the protection of personal information within its organization and process requests (such as access and correction requests) received from individuals who wish to exercise their rights under the Mexican Law.

Data Security. The Regulations, issued in 2011,[29] define what constitutes physical, technical and administrative measures and, in particular, require: the establishment of an internal supervision and monitoring system; implementation of a training program for personnel to educate and generate awareness about their obligations to protect personal information; and external inspections or audits to check compliance with

[25] The Dominican Law is available, in Spanish, at http://www.mofo.com/files/PrivacyLibrary/3983/Ley_172_13_Proteccion_Datos_Caracter_Personal.pdf.

[26] The Mexican Law is available, in English, at http://www.mofo.com/files/Uploads/Documents/FederalDataProtectionLaw2010.pdf (9 PVLR 1016, 7/12/10).

[27] The website address of the Mexican DPA is http://ifai.org.mx/.

[28] The Guidelines are available, in Spanish, at http://abcavisosprivacidad.ifai.org.mx/PDF/El%20ABC%20del%20Aviso%20de%20Privacidad.pdf.

[29] The Regulations are available, in Spanish, at http://bit.ly/1yUor6A (11 PVLR 41, 1/2/12).

privacy policies. The list of security measures must be updated when security improvements or changes are made or there are breaches of the systems. In addition, the organization is encouraged to consider undertaking a risk analysis of personal information to identify dangers and estimate the risks for the personal information, conduct a gap analysis and prepare a work plan to implement the missing security measures arising from the gap analysis.

Whenever there is a security violation involving personal information, the DPA may take into account the organization's compliance with DPA recommendations to determine the attenuation of the corresponding sanction.

Data Security Breach Notification. Security breaches that occur ''at any stage of processing that materially affect the property or moral rights'' of the individual must be reported to the individual by the organization so the individual can take appropriate action to protect his or her rights. The Mexican Law does not require notice to any public authority or regulator.

NICARAGUA

Nicaragua enacted the Law on Personal Data Protection March 21, 2012 (Act No. 787) and the Regulation of the Law on Personal Data Protection (Decree No. 36-2012) (Nicaraguan Law) Oct. 17, 2012.[30] The Nicaraguan Law protects the personal information of natural and legal persons in private and public databases.

In Brief. *The Nicaraguan Law restricts cross-border transfers and requires registration; however, the registration procedure is not yet established. Data security, breach notification and the appointment of a DPO are not required. Unlike other laws in the region, the Nicaraguan Law has a provision of the right to ''digital oblivion.''*

Special Characteristics

Data Protection Authority. The Nicaraguan Law calls for the creation of a Directorate for Personal Data Protection within the Ministry of Finance that will be responsible for the regulation, supervision and protection of the processing of personal information; however, as of March 2015, the Directorate has not yet been established. The Directorate will be responsible for a wide range of data protection-related activities, including issuing regulations, monitoring compliance and imposing administration sanctions in the event of violations.

Cross-Border Transfers. The assignment and transfer of personal information to countries or international organizations that do not provide adequate security and protection for personal information are prohibited except in very limited circumstances, such as where:

- the transfer is for the purposes of international judicial cooperation;
- the exchange of personal information is for health matters;
- the transfer is necessary to carry out epidemiological investigations, wire transfers or exchanges;
- the transfer is required by law;
- the transfer is agreed upon under any international treaties ratified by Nicaragua; or
- the transfer pertains to international cooperation with intelligence agencies or to criminal matters covered by specified laws.

Such transfers must be carried out at the request of a legally authorized person; the request must state the object and purpose of the intended processing; the organization must comply with the data security and confidentiality measures and verify that the receiving organization complies equally with these measures; and the individual must be informed about and consent to the transfer by the organization and the intended purposes of the processing.

Right to Digital Oblivion. The Nicaraguan Law is one of the first laws to include the right to be forgotten, which has been so controversial in the EU. In particular, the individual has the right to request that social networks, browsers and servers suppress or cancel his or her personal information contained in their databases. In the case of databases of public and private institutions that offer goods and services and collect personal information for contractual reasons, individuals may request that their personal information be canceled once the contractual relationship ends. This provision is not particularly detailed, and it is not clear how organizations will implement these obligations.

PERU

The Law for Personal Data Protection (Peruvian Law), which protects the personal information of natural persons processed by public and private sector organizations, entered into force July 4, 2011; however, many of the provisions and its Regulations did not become effective until May 2013.[31] Organizations had until March 2015 to conform their existing personal data banks to the Peruvian Law.

In Brief. *The Peruvian Law requires registration and restricts cross-border transfers. The DPA has also established data security breach notification requirements. There is no obligation to appoint a DPO.*

Special Characteristics

Data Protection Authority. The Peruvian Law established the National Authority for Protection of Personal Data to oversee compliance and, in particular, administer and keep up-to-date the National Register of Personal Data Protection, hear and investigate complaints lodged by individuals, issue provisional and/or corrective measures and impose administrative sanctions in cases of violations.[32]

Cross-Border Transfers. Cross-border transfers of personal information are allowed if the recipient has adequate data protection as may be determined by the DPA. Thus far, the DPA has not issued a list of adequate recipients. The Peruvian Law provides certain excep-

[30] The Nicaraguan Law is available, in Spanish, at http://bit.ly/1ykuvVH. The Regulation is available, in Spanish, at http://bit.ly/1FOip7k.

[31] The Peruvian Law is available, in Spanish, at http://www.minjus.gob.pe/wp-content/uploads/2013/04/LEY-29733.pdf (12 PVLR 529, 3/25/13). The Regulations are available, in Spanish, at http://www.minjus.gob.pe/wp-content/uploads/2013/03/Leydeprotecciondedatos.pdf.

[32] The website address of the Peruvian DPA is http://www.minjus.gob.pe/proteccion-de-datos-personales.

  PVLR ISSN 1538-3423

tions to this provision, including where the transfer of personal information is necessary to complete a contract to which the individual whose information is being transferred is a party; where the individual has given consent; or where otherwise established by regulation issued under the Peruvian Law.

The Regulations additionally provide that cross-border transfers are permitted when the importer assumes the same obligations as the exporting organization. The exporter may transfer personal information on the basis of contractual clauses or other legal instruments that prescribe at least the same obligations to which the exporter is subject as well as the conditions under which the individual consented to the processing of his or her personal information. Therefore, if a contract is in place, consent or one of the other legal bases listed above would not be required.

Authorization for cross-border transfers is not required; however, the organization and the service provider may request the opinion of the DPA as to whether the proposed transfer of personal information cross-border meets the provisions of the Peruvian Law.

Data Security Breach Notification. The Peruvian Law itself does not impose data security breach notification requirements; however, it authorizes the DPA to establish the security requirements and conditions to be met by data controllers. In October 2013, the DPA issued an Information Security Directive that instructs data controllers to notify individuals of ''any incidents that significantly affect their proprietary or moral rights.''[33]

Registration. All organizations must register with the DPA. In addition, organizations that voluntarily adopt codes of conduct to govern their transfers to affiliated entities must register them with the DPA.

URUGUAY

Law No. 18.331 on the Protection of Personal Data and Habeas Data Action (Uruguayan Law), enacted in 2008 and amended in 2010, regulates the processing of personal information of natural and legal persons by both the public and private sectors.[34] Uruguay was the second country in South America to be recognized by the EU as providing an adequate level of protection for personal information transferred from the EU/EEA (11 PVLR 1369, 9/10/12).

Uruguay was the second country in South America to be recognized by the EU as providing an adequate level of protection for personal information transferred from the EU/EEA.

In Brief. *The Uruguayan Law requires data security breach notification and registration and restricts cross-border transfers to countries that do not provide adequate protection. There is no requirement to appoint a DPO; however, the person responsible for the database is liable for violations of the provisions of the law, and his or her name will be identified in the registration.*

Special Characteristics

Data Protection Authority. The Regulatory and Control Unit for the Protection of Personal Data was created as an entity decentralized from the Agency for the Development of Government of Electronic Management and Information Society and Knowledge (AGESIC).[35]

Cross-Border Transfers. The transfer of personal information of any kind to countries or international organizations that fail to provide adequate levels of protection according to the standards of regional or international law in this area is prohibited except where the following cases apply:

- international judicial cooperation, according to the relevant international instrument, whether treaty or convention, subject to the circumstances of each case;
- exchange of medical data, when necessary for the treatment of the sick person and due to reasons of public health or hygiene;
- bank or stock exchange transfers, in regard to the corresponding transactions and pursuant to the applicable legislation;
- agreements within the framework of international treaties to which the Republic of Uruguay is a party; and
- international cooperation between intelligence agencies fighting against organized crime, terrorism and drug trafficking.

It also is possible to make international transfers of data in the following cases:

- the interested party has given his or her consent to the proposed transfer;
- the transfer is necessary for the execution of a contract between the interested party and the person responsible for the processing or to implement pre-contractual measures taken at the interested party's request;
- the transfer is necessary to execute an agreement entered into now or hereafter on behalf of the interested party, between the person responsible for the processing and a third party;
- the transfer is necessary or legally required to safeguard an important public interest, or for the recognition, exercise or defense of a right in a legal procedure;
- the transfer is necessary for safeguarding the vital interests of the interested party; or
- the transfer is effected from a record which, by virtue of legal or regulatory provisions, is designed to provide information to the public and is open to

[33] The Information Security Directive is available, in Spanish, at http://www.minjus.gob.pe/wp-content/uploads/2014/02/Cartilla-de-Directiva-de-Seguridad.pdf.

[34] The Uruguayan Law is available, in Spanish, at http://www.presidencia.gub.uy/_web/leyes/2008/08/CM524_26%2006%202008_00001.PDF (7 PVLR 1410, 9/29/08).

[35] The website address of the Uruguayan DPA is http://www.datospersonales.gub.uy.

consultation by the general public or any person who can prove a legitimate interest, provided that the conditions established by law for consultation are met in each particular case.

Regardless of the cases listed above, the DPA may authorize a transfer or a series of transfers of personal information to a third country that does not guarantee an adequate level of protection when the person responsible for the processing offers sufficient guarantees regarding the protection of privacy, fundamental rights and freedoms of individuals as well as to the exercise of the corresponding rights.

Such guarantees may arise from appropriate contractual clauses.

Data Security Breach Notification. When the data controller or the data processor realizes that there has been a data security breach that could affect the individual's rights in a significant way, the data controller or the data processor must inform the individual.

Registration. All organizations that create, modify or eliminate databases of personal information must register their databases.

COUNTRIES WITH PRIVACY LAWS	REGISTRATION REQUIREMENT	DPO REQUIRED[1]	CROSS-BORDER LIMITATIONS	DATA SECURITY BREACH NOTIFICATION REQUIREMENT[2]
LATIN AMERICA & CARIBBEAN (13)	**6**	**3**	**9**	**5**
Argentina	**Yes**	**Yes**	**Yes**	No
Aruba	No	No	**Yes**	No
Bahamas	No	No	No	No
Chile	No	No	No	No
Colombia	**Yes**	**Yes**	**Yes**	**Yes**
Costa Rica	**Yes**	No	No	**Yes**
Curacao	No	No	**Yes**	No
Dominican Republic	No	No	**Yes**	No
Mexico	No	**Yes**	No	**Yes**
Nicaragua	**Yes**	No	**Yes**	No
Peru	**Yes**	No	**Yes**	**Yes**
Trinidad & Tobago (law not yet fully in force)	No	No	**Yes**	No
Uruguay	**Yes**	No	**Yes**	**Yes**

[1] In some jurisdictions, the appointment of a DPO may exempt the organization from its registration obligations.

[2] This chart identifies only those jurisdictions that have enacted legally binding data breach notification requirements. It does not reflect the local notification practices or the DPA's expectations about whether organizations should provide notice. Consequently, organizations should consider a variety of factors, not just whether the rules are legally binding.

PVLR ISSN 1538-3423