Bloomberg Law

Privacy and Security Law Report®

Data Protection

In this first article of a four-part series on the status of international data protection laws, the author explores developments in the non-U.S. Western Hemisphere (Latin America, the Caribbean, and Canada), where 17 jurisdictions now have comprehensive data protection laws.

A Look at New Trends: Data Privacy Laws in the Western Hemisphere (Latin America, Caribbean and Canada) Continue to Evolve

By Cynthia Rich

Introduction and Region at a Glance

Seventeen jurisdictions in the Western Hemisphere region (Latin America, the Caribbean, and Canada) now have comprehensive privacy laws including: Antigua and Barbuda, Argentina, Aruba, Bahamas, Bermuda, Canada, Chile, Colombia, Costa Rica, Curacao, Dominican Republic, Mexico, Nicaragua, Peru, St. Maarten, Trinidad and Tobago (currently, the only provisions in force pertain to the establishment of the data protection authority), and Uruguay. Saint Lucia adopted legislation in 2011, but the law has not yet gone into effect. The laws in three countries (Argentina, Canada, and Uruguay) have been deemed by the European Commission to provide adequate protection.

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

Other countries, such as Brazil, Ecuador, El Salvador, Jamaica, and Panama, 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, earlier this year, the Chilean President sent new draft legislation to the Senate that, if enacted, would significantly amend the country's 1999 data privacy law. Similarly, Argentina is working on new legislation that would amend its current law, while Costa Rica and Peru recently enacted amendments to their existing laws.

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

Developments and Trends

Amendments to Existing Privacy Laws In the past year, four countries with established privacy laws in the region (Argentina, Chile, Costa Rica, and Peru) have either amended or are in the process of amending their laws. With the impending implementation of the General Data Protection Regulation (GDPR) in the European Union, governments in these countries are trying to bolster their chances of having their laws deemed adequate by the European Commission.

For example, in February of this year, the Argentine data protection authority (Argentine DPA) held a public consultation on a draft law that is heavily based on the

 ISSN 1538-3423

European General Data Protection Regulation (GDPR). Proposed changes include: elimination of the registration requirement; redefinition of data subjects to exclude legal entities; addition of new definitions such as for biometric and genetic data; addition of new legal bases for processing personal information such as legitimate interests; revised rules for international transfers (including binding corporate rules); new provisions on cloud computing, data breaches, accountability, and privacy by design; and new mandatory data protection officer (DPO) and privacy impact assessment (PIA) requirements. The Argentine DPA also issued in November 2016 its list of countries that provide adequate protection and new model clauses and guidance on cross-border transfers issued. While the two sets of model clauses (one for controller-controller transfers and one for controller-processor transfers) resemble the EU model clauses, there are many differences as well, some of which exceed EU requirements.

In March of this year, the Chilean President sent new draft legislation to the Senate that, if enacted, would significantly amend the country's existing data privacy law. The government's proposed amendments introduce new data privacy principles (including the right to data portability) and establish new requirements for consent, use of sensitive data (including biometric and children's data), international data transfers, security, and data breach notification. In addition, the legislation provides for the creation of a data protection authority with the authority to impose significant fines for law violations.

Last December, Costa Rica enacted significant changes to its law that, among other things, eliminated the controversial Super User provision which gave the data protection authority the right to gain unrestricted access to registered databases. The amendments also clarified that databases used for internal purposes, such as human resources databases, including those shared with affiliated entities, do not need to be registered with the regulator, and that sharing of personal information with affiliated entities and agents does not constitute a transfer that would trigger the need for consent.

Peru also enacted amendments in January of this year that modified obligations in several areas, such as notice, consent, and registration. In particular, the law now has new exceptions for processing (including sharing within an affiliated group of companies) without the need for consent when such processing is done in connection with anti-money laundering and terrorism financing as well as for other regulatory compliance purposes. In addition, the amendments eliminated the registration requirement for codes of conduct of database owners and data processors.

There were other noteworthy developments this past year in three other countries in the region: Canada, Colombia, and Mexico. In March 2016, the Canadian government issued a consultation paper seeking comments on the new data breach regulations that will be issued under the revised Personal Information Protection and Electronic Documents Act (PIPEDA). When PIPEDA was revised in June 2015 with the enactment of the Digital Privacy Act, a breach notification reporting requirement was added; however, the entry into force of this requirement was delayed pending the issuance of the regulations. Canada's Ministry of Innovation, Science, and Economic Development intends to publish regulations this year that will be subject to public consultation and a transition period before the regulations enter into force.

In Colombia, the data protection authority is working on developing standards to determine whether a third country ensures an adequate level of data protection. Earlier this year, the DPA issued for public comment its draft adequacy standards as well as its proposed list of countries that provide adequate protection and additional rules for transfers to inadequate countries. Lastly, in late January 2017, Mexico enacted a data privacy law regulating the public sector use of information.

New Data Privacy Laws Enacted and Under Development Bermuda became the latest country in the region to enact a comprehensive privacy law in August 2016. The Personal Information Protection Act, 2016 (PIPA), which does not go into effect until 2018, applies to processing of personal information by public and private sector organizations and, in addition to the common privacy law requirements, imposes obligations with respect to international transfers, data breach notification, and the appointment of a data protection officer.

Elsewhere in the region, efforts to enact data privacy legislation continue in fits and starts. For example, Brazil has made several unsuccessful attempts over the past few years to adopt legislation. Currently there are draft competing laws pending in both houses of the Brazilian Congress. Similarly, enactment of legislation in the Cayman Islands has been delayed yet again. The government has attempted to pass legislation twice, but those efforts failed to progress in Parliament because of concerns from the business community that the cost of implementing the law's requirements would be too costly and concerns that it would not satisfy EU adequacy requirements. The government reintroduced the legislation in March 2017 but no action was taken by the time the Parliament was dissolved prior to the upcoming May elections.

The President of Ecuador's National Assembly introduced draft legislation on the Protection of Privacy and Personal Data in late July 2016, and debate on the legislation began in December. However, the legislature did not act on the proposed legislation prior to the national elections in February 2017, so action on this or any other privacy bill will likely not take place until mid to late 2017.

In El Salvador, a preliminary draft ''Data Protection Law'' is currently being studied by a technical panel composed of representatives from the Ministry of Economy, the Institute for Access to Public Information (IAIP), and the National Registry of Natural Persons.

In Jamaica, the Minister of Science, Energy, and Technology announced in April 2017 that the government intends to present to Parliament its proposed Data Protection Act within three months.

In Panama, the government, the National Authority of Transparency and Access to Information (ANTAI), held a public consultation in July 2016 on a draft Data Protection Bill. A revised version, published in September, was submitted to the National Assembly in February 2017 where it is expected to take about two years to debate and enact.

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

  PVLR ISSN 1538-3423

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 DPAs in Colombia, Mexico, and Peru have been the most active in issuing fines, some of which have been quite high.

For example, the Mexican DPA imposed a total of 93 million Mexican pesos ($4.9 million) in fines in 2016, mostly in the financial and insurance services, mass media, and retail sectors. The most common violations cited were: failure to comply with the data processing principles (legality, information, accountability, loyalty, and consent), failure to obtain explicit consent to collect or transfer personal information, and deficient privacy notices. The largest fines imposed todate on a single corporation were three fines amounting to MXN 32 million ($2 million) that were issued to banking institution Grupo Financiero Banorte in 2015 for, among other things, collecting sensitive personal information without obtaining the individual's express written consent, maintaining personal databases that contain present and future health data of persons without a legal justification to process this information, and failing to provide notice.

In 2016, the Colombian DPA fined Colmedica Medicina Prepagada S.A. 1.03 billion Colombian pesos ($ 345,000) for its failure to adequately protect personal data and to report security incidents to the DPA. It also fined a bank COP 276 million ($94,000) for sending unauthorized marketing communications. Total fines issued in 2016 amounted to approximately COP 2.2 billion ($ 750,000), compared to twice that amount the preceding year. In 2016, the Peruvian DPA concluded the first case involving the ''right to oblivion'' under the data privacy law (i.e., the right to delete all or part of an individual's personal information from an organization's database). In this case, which began in late 2015, a Peruvian citizen, who had been accused and then subsequently acquitted of a crime, sought without success to expunge news reports about the criminal charges from various websites and Alphabet Inc. Google's search results. The DPA fined Google 256,750 Peruvian sol ($79,000) for violating an individual's ''right to oblivion'' and ordered Google to hide certain search results. The DPA ruled that Google was required to comply with Peruvian laws even though it is a foreign company because it processed personal information of Peruvians and the information was accessible from Peru. This fine appears to be the largest fine todate, slightly exceeding the next largest fine of $78,600 fine, which was imposed on the Peruvian company DATOSPERU.ORG in 2014 for publishing sensitive personal information of two citizens on its Web page without their consent.

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 when 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. In addition, there is a provision that allows the government to enforce against offshore businesses that collect, maintain, or store data from Brazilian users.

Common Elements Found in Latin American Laws

Notice All of the laws in this region 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 Canada and 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. The Argentina requirements are quite similar to Spain.

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

For example, two-thirds of the countries in this region restrict cross-border transfers of personal informa-

tion to countries that do not provide adequate protection. However, unlike the European approach (and more like the approach in countries such as Kazakhstan, Singapore, or South Korea), 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 DPAs haven't specified what must be contained in these contracts or rules. Most of the laws in this region 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: more than one-third of the countries require registration and notification in the event of a data breach and almost one-quarter require the appointment of a DPO. In addition, approximately one-half of the laws in the region require that access and/or correction requests be responded to within 10 days or less (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 Peru, provide 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 country obligations in this region.

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.

Country-by-Country Review of Differences

ANTIGUA AND BARBUDA

The Data Protection Act (Antigua and Barbuda Law), enacted in 2013, protects personal data of natural persons and legal entities that are processed by public and private sector organizations.

In Brief The Antigua and Barbuda Law does not require database registration; impose mandatory DPO, data security breach, or detailed security obligations; or restrict cross-border transfers.

Special Characteristics

Data Protection Authority The Information Commissioner pursuant to the Freedom of Information Act 2004 is responsible for enforcement of the Antigua and Barbuda Law. There is no website available for the Information Commissioner.

Consent Consent is required to process personal data unless an exception applies (e.g., contractual necessity, legal obligation, or vital interests). Explicit consent is required to process sensitive personal data.

Definition of Personal Data Personal data of natural and legal persons are defined as any information processed in the context of ''commercial transactions.'' Such commercial transactions, whether contractual or not, include any matters relating to the supply or exchange of goods or services, investments, financing, banking, and insurance. Sensitive personal data are defined as any personal data relating to the physical or mental health or condition of a data subject, sexual orientation, political opinions, religious beliefs, or commission of criminal offenses (proven or alleged).

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. Argentina was the first country, and currently only one of two countries in Latin America, to be recognized by the European Union as providing an adequate level of protection for personal information transferred from the EU/European Economic Area.

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.

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. In November 2016, the DPA recognized the following countries as providing adequate protection: EEA member states, Switzerland, Guernsey, Jersey, Isle of Man, Faroe Islands, Canada (private sector only), Andorra, New Zealand, Uruguay, and Israel (automatically processed data only).

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 issued two sets of model clauses (one for controller-controller transfers and one for controller-processor transfers)

  PVLR ISSN 1538-3423

that resemble the EU model clauses; however, some of the provisions actually exceed EU requirements.

Data Security After the Argentine Law was enacted, regulations imposing additional security requirements were issued. *See* Disposition 11/2006 (Security Measures), Sept. 20, 2006. 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.

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. 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.

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.

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.

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.

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. 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 of; or accidental loss or destruction of personal information.

BERMUDA

The Personal Information Protection Act 2016 (Bermuda Law), enacted in August 2016, protects the personal information of natural persons and applies to processing of such data by both the public and private sectors. The Bermuda Law does not go into effect until 2018.

In Brief The Bermuda Law imposes mandatory DPO and data security breach obligations and restricts cross-border transfers; however, database registration is not required.

Special Characteristics

Data Protection Authority The Office of the Privacy Commissioner, which is not yet established, will be responsible for monitoring compliance with the law, including conducting investigations, issuing guidance, and working with law enforcement authorities to enforce the law. The Commissioner will also be responsible for investigating and attempting to resolve complaints received from individuals. Legislation paving the way for the appointment of the Commissioner came into force in December 2016.

Cross-Border Transfers Before transferring personal information overseas to a third party, a transferring organization must assess the level of privacy protection provided by the overseas third party. When assessing the level of protection, the organization must consider the level of protection afforded by the law applicable to such overseas third party and the Minister, on the rec-

ommendation of the DPA, may designate any jurisdiction as providing a comparable level of protection. Adoption of a certification mechanism recognized by the DPA is one way to demonstrate comparable protection. If the level of protection is not comparable, then the organization must employ contractual mechanisms, corporate codes of conduct including binding corporate rules, or other means to ensure that the overseas third party provides a comparable level of protection.

When an organization transfers personal information to an overseas third party, the organization remains responsible for compliance with the Bermuda Law.

Data Protection Officer An organization must designate a DPO who will have primary responsibility for communicating with the DPA. The designated privacy officer may delegate his duties to one or more individuals. A group of organizations under common ownership or control may appoint a single DPO provided that a DPO is accessible from each organization.

Data Security Breach Notification In case of a breach of security leading to the loss or unlawful destruction or unauthorized disclosure of, or access to, personal information that is likely to adversely affect an individual, the organization responsible for that personal information must, without undue delay, notify the DPA of the breach and then any individual affected by the breach.

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.

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.

CANADA

The Personal Information Protection and Electronic Documents Act regulates the collection, use, and disclosure of personal information of natural persons by private sector organizations for commercial purposes, with limited exceptions (e.g., where the organization is handling personal information in a province with substantially similar provincial legislation and the organization is provincially regulated).

In the context of an employment relationship, the collection, use, and disclosure of employees' personal information by an employer is covered only where the employer is a private-sector Federal Work, Business or Undertaking, meaning a federally regulated entity (e.g., organizations in the transportation, communications, broadcasting and banking sectors). Canada is regarded as providing an adequate level of protection for personal data transferred from the EU/EEA.

In Brief The Canadian Law requires the appointment of a DPO and will require breach notification once regulations implementing the July 2015 amendments are issued. However, there are no cross border restrictions or special security or registration requirements.

Special Characteristics

Data Protection Authority The Privacy Commissioner of Canada (Canadian DPA) is responsible for investigating complaints, conducting audits, and pursuing court action under two federal laws. It also publicly reports on the personal information-handling practices of public and private sector organizations and promotes public awareness and understanding of privacy issues. The DPA does not have the authority to order compliance, award damages, or levy penalties.

Cross-Border Transfers There are no express limitations in the Canadian Law on cross-border transfers. In fact, the Canadian Law does not distinguish between domestic and international transfers of data. However, any organization that has transferred personal information to a third party (including an affiliate) for processing generally remains responsible for that personal information. The organization that transfers personal information to any foreign service provider must use contractual or other means to provide comparable level of protection while personal information is in possession of foreign entity.

Data Breach Notification In June 2015, Parliament passed amendments to the Canadian Law requiring mandatory breach notification, which will come into force once the implementing regulations are issued. Organizations will be required to report to the Commissioner and notify affected individuals of a breach where the breach poses a ''real risk of significant harm'' to affected individuals. Organizations must also notify government institutions and other organizations in prescribed circumstances, including where the organization believes that the government institution or other organization may be able to reduce or mitigate the risk of harm to affected individuals. Until these amendments come into force, there is currently no legal obligation to give notice in the event of a data security breach; however, the DPA has issued voluntary breach notification guidelines.

The Guidelines recommend that notice be given when there is unauthorized access to or collection, use, or disclosure of personal information that creates a risk of harm to the individual, based on a case-by-case basis approach. The organization that has the direct relationship with the individual customer, client, or employee should notify the affected individuals, including when the breach occurs by a third-party service provider, unless in the given circumstances direct notice by the third-party service provider is more appropriate.

Data Protection Officer Organizations must appoint an individual or individuals who are accountable for the organization's compliance with the Canadian Law. Although other individuals within the organization may be responsible for the day-to-day processing of personal information, accountability rests with the designated individual.

COLOMBIA

Enacted in October 2012, Law No. 1581 ''Introducing General Provisions for Personal Data Protection'' (Co-

  PVLR ISSN 1538-3423

lombian 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. The Colombian Law is intended to complement a law enacted in 2008 that applies to personal credit information only.

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.

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 or 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 non-adequate 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 or determine whether a third country provides adequate protection will be addressed in standards to be issued by the DPA. In February 2017, the DPA issued for public comment its draft adequacy standards as well as its proposed list of countries that provide adequate protection and additional rules for transfers to inadequate countries.

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 Organizations and service providers that carry out processing of personal information in Colombia must register with the DPA. It is quite unusual to require service providers to file registrations with the DPA. The National Registry was officially launched in November 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. It applies to automatic and manual processing of personal information of natural persons by both public and private entities. Last December, Costa Rica enacted significant changes to its law that, among other things, eliminated the controversial Super User provision that gave the DPA the right to gain unrestricted access to registered databases. The amendments also clarified that databases used for internal purposes, such as human resources databases, including those shared with affiliated entities, do not need to be registered with the regulator, and that sharing of personal information with affiliated entities and agents does not constitute a transfer that would trigger the need for consent.

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

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 results 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. However, human resources databases, including those shared with affiliated entities, do not need to be registered with the DPA.

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. 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,or 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.

Cross-Border Transfers Personal information may only be transferred to a country outside the Kingdom of the Netherlands (Editor's note: the Kingdom of the Netherlands consists of the Netherlands, Aruba, Curacao, and Sint Maarten) 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 that 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) took effect in December 2013. 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.

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 Transfer 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 acknowledgment, 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, 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.

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.

Notice In 2013, the DPA issued Guidelines that provide for three different types of privacy notices: comprehensive, simplified, and short. A comprehensive pri-

  PVLR ISSN 1538-3423

vacy 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 doesn't 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, 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 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 in March 2012 (Act No. 787) and the Regulation of the Law on Personal Data Protection (Decree No. 36-2012) (Nicaraguan Law) in October 2012. 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 May 2017, 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 natu-

ral persons processed by public and private sector organizations, entered into force in July 2011; however, many of the provisions and its Regulations did not become effective until May 2013. Organizations had until March 2015 to conform their existing personal data banks to the Peruvian Law. The Peruvian Law was recently amended in January of 2017 to modify obligations in several areas, such as notice, consent, and registration.

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.

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 hasn't issued a list of adequate recipients. The Peruvian Law provides certain exceptions 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.''

Registration All organizations must register with the DPA.

ST. MAARTEN

The Personal Data Protection National Ordinance (St. Maarten Law), enacted in 2010, regulates the processing of personal information of natural persons by both the public and private sectors.

In Brief The St. Maarten Law restricts cross-border transfers but does not impose registration, data security breach notification or DPO requirements.

Special Characteristics

Data Protection Authority The Personal Data Protection Supervisory Committee is responsible for supervising compliance with the Ordinance.

Cross-Border Transfers Personal data may be sent to another country only if that country guarantees an appropriate level of protection; otherwise, transfers to a country without an appropriate level of protection may take place only if:

- the individual has granted unambiguous consent for this;
- the transfer is necessary to carry out a contract between the individual and the organization, or to take pre-contractual measures in response to a request by the individual and that are necessary for the contracting of an agreement;
- the transfer is necessary for the contracting or execution of an agreement contracted or to be contracted between the Responsible Party and a third party, in the interest of the Individual;
- the transfer is necessary due to a serious general interest or for the establishment, exercise, or the defense of any right in court;
- the transfer is necessary to protect a vital interest of the individual; or
- the transfer takes place from a register installed by law and that can be viewed publicly, or by any person that can invoke a justified interest, to the extent that, in the case concerned, the statutory requirements for viewing have been met.

Data transfers are also allowed when the Committee issues a permit for transfers to a country that does not provide assurances of an appropriate level of protection. The provisions necessary to secure the protection of privacy and the fundamental rights and freedoms of persons, as well as the exercise of the associated rights, need to be attached to the permit.

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. 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.

  PVLR ISSN 1538-3423

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).

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 precontractual 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 that, by virtue of legal or regulatory provisions, is designed to provide information to the public and is open to 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.

Links to all of the data privacy laws and data protection authorities discussed in this article are available in Morrison & Foerster's online Privacy Library at http://www.mofoprivacy.com.