Bloomberg BNA

Privacy and Security Law Report®

Privacy in Latin America

BY CYNTHIA RICH, MARIAN WALDMANN AGARWAL, AND MIRIAM WUGMEISTER

The privacy landscape in Latin America[1] is undergoing significant changes. With the enactment or implementation of laws in Colombia, Costa Rica, Nicaragua, and Peru, there are now eleven countries in Latin America that have adopted omnibus data privacy legislation: Argentina, Bahamas, Chile, Colombia, Costa Rica, Mexico, Nicaragua, Peru, Saint Lucia,[2] Trinidad and Tobago,[3] and Uruguay. In addition, Brazil is considering a data protection law.

Unlike the European Union member state laws which are all based on a common directive, the Latin American laws vary significantly from each other. All of these laws are based on the core data protection principles, but their implementation and focus are quite different from each other and from laws found in other parts of the world. In addition, unlike the newer laws being adopted in Asia (11 PVLR 1798, 12/17/12), the new laws in Latin America require registration with the data protection authority, and they do not contain detailed security obligations. However, like the new laws in Asia and the existing laws in Europe, the Latin American laws impose cross-border restrictions. Organizations doing business in Latin America should pay attention to these laws as they really differ from laws in other regions, and compliance programs that comply with only EU obligations will run afoul of many of the Latin American country obligations.

This article provides an overview of the requirements set out by the recently adopted laws in Latin America.

[1] This article uses the term ''Latin America'' in its broadest sense, ''all of the Americas [south] of the United States.'' *Latin America*, Merriam-Webster, http://www.merriam-webster.com/dictionary/latin%20america (last visited Jan. 2, 2013).

Cynthia Rich is a senior international policy analyst in 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. Miriam Wugmeister is a partner at firm's New York City office, where she is chair of the firm's Global Privacy and Data Security Group. Marian Waldmann Agarwal is an associate at the New York City office and a member of the firm's Global Privacy and Data Security Group. Global Employee Privacy and Data Security Law, Second Edition, written by Morrison & Foerster, edited by Wugmeister and partner Christine E. Lyon, and published by Bloomberg BNA, is now available for download on the iPhone, iPad, and iPod touch.

COLOMBIA

Overview

Two years after the Colombian Congress approved an omnibus data protection law, the law has finally

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

[3] On Jan. 6, 2012, Trinidad and Tobago adopted a Data Protection Act, 2011; although, currently, the only provisions in force pertain to the establishment of the data protection authority.

 ISSN 1538-3423

been officially enacted. Law No. 1581 ''Introducing General Provisions for Personal Data Protection'' (the 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.[4] The Colombian Law is intended to compliment a law enacted in 2008 that applies to personal credit information only. Organizations have six months (until April 17, 2013) to come into compliance with the Colombian Law.

The Colombian Law applies to processing carried out on Colombian territory, and to data controllers (organizations) and service providers not established on Colombian territory that are subject to Colombian legislation under international rules and treaties. The Colombian Law does not apply to databases or files in which financial, credit, commercial and services information is held or census databases and files.

Establishment of Data Protection Authority

In the next six months, the government is required to establish a data protection authority (the Colombian DPA) within the Superintendence of Industry and Commerce that will be responsible for ensuring compliance with the Colombian Law. In particular, it is authorized to carry out investigations on the basis of complaints or on its own initiative. The Superintendence will also be responsible for maintaining the National Registry of Databases, recommending amendments to regulations to bring them into line with technological advances, and collaborating with international or foreign entities when the rights of individuals are affected outside the Colombian territory.

Appointment of a Data Protection Officer

There is no statutory requirement to appoint a data protection officer; however, implementing regulations have not yet been issued and may address this issue.

Notice and Consent

There is a general obligation to give notice under the ''Principle of Purpose.'' In particular, individuals must be informed about what personal information is being processed, the purposes of that processing, the fact that it is optional to answer questions about sensitive information or data about children, their rights under the Colombian Law (such as access and correction rights), and the name and address of the organization. Notice must be provided whenever the individual's prior and informed authorization (consent) is required to process personal information. (Authorization is required to process any personal information unless an exception applies.)

The individual's prior, express and informed consent is required to process personal information (explicit consent is required for sensitive information) unless one of the very limited exceptions applies. The individual has the right to revoke consent where the processing of his/her personal information does not respect applicable constitutional and legal principles, rights, and guarantees.

[4] 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).

Data Security

The organization and service provider must ensure that information is handled with technical, human and administrative means that guarantee the security of records and protect personal information and records against alteration, loss, unauthorized consultation or use or fraudulent access. Where processing is carried out by a service provider on behalf of the organization, the organization must require that the service provider comply with security requirements and privacy conditions to ensure security and confidentiality of the data processed.

Data Integrity and Data Retention

Personal information must be truthful, complete, correct, provable, and comprehensible and must be kept up-to-date. Processing of partial, incomplete, fragmented, or misleading data is prohibited. No specific data retention obligations are specified; however, implementing regulations have not yet been issued and may further address this issue.

Access and Correction Rights

The individual has the right at any time, free of charge, and without restrictions, to obtain from the organization or service provider confirmation as to whether his/her personal information is processed, and information about the processed information, including its purposes of use. The organization or service provider must respond to such requests within 10 business days from the date of receipt of the request. This is a very short time period.

Where the individual determines that the information in a database should be corrected, updated or deleted, or when he/she notices any presumed noncompliance with the Colombian Law, the individual may submit a complaint to the organization or service provider. In response to a complaint, the organization or service provider must note in the record that a complaint is in progress, and such notation must be maintained until the complaint is resolved within a 23-day period.

Cross-Border Data Transfer

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 and unequivocal consent to the transfer or one of the following other legal bases applies:

- the transfer consists of the exchange of medical data required to treat the individual for public health or hygiene reasons;
- the transfer is a bank or stock exchange transfer, according to applicable legislation;
- the transfer is agreed upon under international treaties to which the Republic of Colombia is a party, based on the principle of reciprocity;
- the transfer is necessary in order to execute a contract between the individual and the organization or in order to take precontractual measures; or
- the transfer is legally required in order to protect a public interest or for the recognition, exercise or defense of a right in a lawsuit.

  PVLR ISSN 1538-3423

The Colombian DPA may approve transfers to non-adequate countries that do not fall under one of the above-listed exceptions. These exceptions are very narrow, and thus consent will be required for most cross-border transfers unless the Colombian DPA expands the list. The Colombian Law contains no exception for transfers to service providers outside or within Colombia. The additional requirements and obligations that must be satisfied before the Colombian DPA may issue such declarations are expected to be addressed in the forthcoming implementing regulations.

Database Registration

Organizations and service providers that carry out processing of personal information in Colombia must register with the Colombian DPA. A record will be entered into the National Registry of Databases, which is available for public consultation. The government has been given until Oct. 17, 2013, to establish the registration procedures and requirements. It is quite unusual to require service providers to file registrations with the data protection authority.

Breach Notification

Both the organization and the service provider must inform the Colombian DPA about any violations of security codes and any risks in the administration of information of individuals. No additional requirements are specified; however, the implementing regulations have not yet been issued and may address this issue in greater detail.

Penalties

The Colombian Law does not impose any criminal sanctions; however, the Colombian Criminal Code includes a set of provisions with criminal penalties regarding the use of personal information and databases. Penalties under the Criminal Code include imprisonment ranging from 48 to 96 months and fines ranging from COP 56,680–566,800 (approximately $31–$315).

With respect to civil and/or administrative penalties, organizations and service providers are liable for fines of up COP 1,133,600 (approximately $630) at the time a sanction is imposed. Fines may be successive for as long as the noncompliance continues. The Colombian DPA may order suspension of activities related to the processing of personal information for up to 6 months, and order compliance actions. In the case of noncompliance with such orders, temporary closure of operations related to processing may be enforced. In addition, individuals have a private right of action under the Colombian Law.

PERU

Overview

On July 3, 2011, Peru published the Law for Personal Data Protection (the Peruvian Law) in the Official Gazette.[5] Some sections of the Peruvian Law took effect the following day, including Title II – the Guiding Principles, and the first paragraph of Article 32 establishing the National Authority for Protection of Personal Data (the Peruvian DPA) as the data protection authority. The remainder of the Peruvian Law will not enter into force until 30 days after the regulations are issued.

The Peruvian Law applies to personal information held in both publicly and privately administered databases, but it does not apply to databases created for personal or family uses. It is based on eight guiding principles common to many other privacy and data security laws with which data controllers and processors must comply: (1) legality; (2) consent; (3) purpose; (4) proportionality; (5) quality; (6) security; (7) availability of recourse; and (8) adequate level of protection.

A final draft version of the regulations was issued Sept. 22, 2012, and public comments were due Oct. 12, 2012.[6] The regulations include, among other things, provisions that allow for the use of digital signatures to satisfy written consent; allow for privacy policies to satisfy information notice requirements; require contractual provisions for cross-border transfers; and place specific requirements on cloud computing service providers.

Establishment of Data Protection Authority

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

Notice and Consent

Individuals must receive notice and be informed of the following prior to the collection of personal information:

(1) the purposes for which the personal information will be processed;

(2) the recipients of the personal information;

(3) the existence of the database in which the personal information will be stored;

(4) the identities and addresses of the controller and any processors;

(5) whether the provision of personal information is required or optional;

(6) intended transfers of personal information (this refers to both national and international data transfers);

(7) the consequences of providing or refusing to provide personal information;

(8) the retention period for personal information; and

(9) the individual's rights, such as access and correction rights.

The Peruvian Law provides that ''prior, informed, express and unequivocal'' consent must be obtained to process personal information unless otherwise pro-

[5] The Law for Personal Data Protection is available, in Spanish, at http://www.jovenesalaobra.gob.pe/Descargas/transparencia/LEY-29733.pdf (10 PVLR 1004, 7/11/11).

[6] The final draft is available, in Spanish, from the Peruvian DPA's website at http://www.minjus.gob.pe/proyecto-de-reglamento-lpd/ .

vided by law. To process sensitive information, consent must also be in writing. As mentioned above, the final draft regulations have clarified that digital signatures will satisfy this written consent requirement.

Consent may not be required in certain circumstances, including, for example, where personal information is intended to be included in publicly accessible sources, where personal information is necessary to perform a contract, and where the information has been anonymized. Consent may be revoked by the individual at any time.

Data Security

Technical, organizational, and legal measures are required to guarantee the security of personal information and protect it from alteration, loss, unauthorized processing, or access. Any party processing personal information—whether the organization or its service provider—must maintain the confidentiality of personal information, even beyond the termination of the relationship between the processor and controller. The Peruvian DPA will establish additional security requirements.

Data Integrity and Data Retention

Personal information that is processed must be accurate and updated.

Personal information should be ''eliminated'' when no longer necessary or relevant for the purposes for which it was collected or when the processing term has ended, unless the information has been anonymized.

Access and Correction Rights

Individuals have the right to access the personal information processed about them, including: (1) how the information was compiled; (2) the purposes for compiling; (3) at whose request the information was gathered; and (4) what transfers have or will be made of the information. This access standard is more detailed and broader than is typically seen in data protection laws. Individuals may also request that personal information be updated, added to, corrected, or deleted (subject to legal limitations) if the information is inaccurate, incomplete, or no longer necessary or relevant for the processing purposes.

The organization is responsible for sharing any updates that are made to personal information with third parties with whom the organization has shared personal information (both with organizations and service providers). The obligation to inform third parties with whom the information has been shared is a new obligation that is beginning to be found in more recently enacted laws.

Further, the organization has an obligation to store personal information in a way that makes it possible for individuals to exercise their rights. No fee can be charged for allowing individuals to exercise these rights unless the regulations state otherwise.

Cross-Border Data Transfer

Cross-border transfers of personal information are allowed if the recipient has adequate data protection as may be determined by the Peruvian DPA. Thus far, the Peruvian DPA has not 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.

Database Registration

The Peruvian Law creates the National Registry of Protection of Personal Data, administered by the National Authority for Protection of Personal Data, that will record all of the public and private databases, the authorizations issued in accordance with the regulations, the sanctions and the corrective or protective measures taken. However, the registration requirement will not become effective until after the regulations are issued and published.

Penalties

The Peruvian DPA is given the right to impose administrative sanctions for violations of the Peruvian Law. Fines may range from 1 UIT to 100 UITs (approximately $1,400–$137,000) and will be capped at 10 percent of the annual gross income received by the violator in the previous fiscal year. Violation of the sanctions imposed may subject the violator to an additional fine. While there are no private rights of action, the individual has the right to be indemnified if he or she is affected as a result of the data controller or data processor violating the Peruvian Law.

COSTA RICA

Overview

Law No. 8968 on the Protection of the Person Concerning the Treatment of Personal Data (the Costa Rican Law) came into force Sept. 5, 2011.[7] It applies to automatic and manual processing by both public and private entities. The Costa Rican Law establishes a data protection authority, the Data Protection Agency of the People (Prodhab), responsible for creating a database registry, ensuring compliance with the law, and issuing implementing regulations. Prodhab, which was officially created March 5, 2012, is in the process of drafting implementing regulations that are expected to be issued this fall. Companies have until March 5, 2013, to bring their practices into compliance with the Costa Rican Law.

Notice and Consent

At the time of collection, organizations must inform individuals of the following:

(1) the existence of the personal information database;

(2) the purposes of data collection;

(3) the recipients of the information as well as those who will have access to the information;

(4) whether the provision of the personal information is required or voluntary;

(5) how the information will be processed;

[7] Law No. 8968 on the Protection of the Person Concerning the Treatment of Personal Data is available, in Spanish, at http://historico.gaceta.go.cr/pub/2011/09/05/COMP_05_09_2011.pdf (10 PVLR 1382, 9/26/11).

  PVLR ISSN 1538-3423

(6) the consequences of refusing to provide data;

(7) individuals' rights; and

(8) the identity and address of the data controller.

Consent is almost always required under the Costa Rican Law. Express consent will be required in written or electronic form to collect, use, and disclose personal information, unless one of the limited exceptions applies.

Processing of sensitive personal information is prohibited unless individuals provide their consent or one of the limited exceptions applies. Exceptions include:

- where necessary to protect the vital interests of the individual concerned or another individual, provided that the individual is physically or legally incapable of providing consent;
- where the processing is carried out by philosophical, religious, trade union-related foundations, associations or organizations in the course of their legitimate activities, as long as they provide appropriate guarantees and the processing relates to their members or people with whom they have frequent contact and the data are not disclosed to third parties;
- where necessary to establish, exercise, or defend individuals' rights in judicial proceedings;
- where the processing relates to information made public voluntarily by the individual concerned; or
- where the processing is required for medical diagnosis, provision of medical care or treatment, or the management of health services.

Information pertaining to credit behavior is governed by rules regulating the National Financial System to guarantee an acceptable level of risk by financial institutions, without impeding the right to informational self-determination.

Data Security

The organization must take technical, physical, and organizational measures to ensure the security of personal information and avoid alteration, accidental or unlawful destruction, loss or unauthorized access, or any violation of the Costa Rican Law. Regulations will establish security requirements.

Data Integrity and Data Retention

Personal information collected must be current, truthful, accurate, and adequate for the purposes for which it was collected. The organization must modify or supplement information that is false or incorrect. Information collected without the informed consent of the individual or data whose collection was prohibited must be removed.

Personal information that is no longer relevant or necessary for the purposes for which it was received and registered must be removed from the database. Personal information may not be kept longer than 10 years after the information was registered unless special legislation provides otherwise. If the information needs to be preserved beyond the stipulated time, it must be anonymized. This obligation to delete data after a specific period of time is very unusual.

Access and Correction Rights

Individuals have the right to access and correct their personal information. Organizations must provide such access rights free of charge within five business days from the date of receipt of the request. Individuals must: be provided with access to their information at reasonable intervals as provided by regulation without delay and free of charge; obtain confirmation about the existence of their data in files or databases; receive written, complete and clear information about the personal information contained in the database, and the purposes for which it was collected and used; and be given an understanding of the system, program, method, or process used to handle their personal information. An explanation of any technical terms used must be provided.

Individuals have the right to have their information corrected, updated, or removed if it has been processed contrary to the provisions of the Costa Rican Law.

Data Transfers

Organizations may only disclose personal information with the explicit consent of the individual and if such transfer is made without violating the principles and rights under the Costa Rican Law. 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. The Costa Rican Law also does not offer any distinction for disclosures to service providers or subcontractors. This provision is also atypical and if not tempered in the regulations may prove particularly difficult for organizations doing business in Costa Rica.

Database Registration

Every database that is established for distribution, promotion or commercialization purposes must be registered with Prodhab.

Penalties

Prodhab can impose sanctions on violators. Violations are divided into three levels of offenses with corresponding levels of sanctions. The most serious offenses may result in a fine of 15 to 30 base salaries and the entity being suspended from using the database for one to six months. A base salary has been defined in Legal Bulletin No. 6 of Jan. 9, 2012, as CRC 360,600(approximately $722). Serious offenses include: (1) the collecting, storing, transmitting, or other processing of sensitive information; (2) obtaining personal information by deception, violence, or threats; (3) unlawfully disclosing personal information that the law requires be maintained confidentially; (4) knowingly providing false information to a third party; (5) processing personal information without registering a database with Prodhab; and (6) transferring an individual's personal information to third countries without the individual's consent.

NICARAGUA

Overview

Nicaragua enacted the Law on Personal Data Protection (Act No. 787) (Nicaraguan Law) March 21, 2012, and the Regulation of the Law on Personal Data Protec-

tion (Decree No. 36-2012) Oct. 17, 2012.[8] The Nicaraguan Law protects personal information of natural and legal persons in private and public databases.

Establishment of a Data Protection Authority

The Nicaraguan Law calls for the creation of a Directorate for Personal Data Protection (the Directorate) within the Ministry of Finance that will be responsible for the regulation, supervision and protection of processing of personal information. 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.

Notice and Consent

Prior to processing personal information, notice must be made available to the individual and include information such as the purposes for which it will be used, the recipients or classes of recipients, contact information for the organization, whether it is voluntary or mandatory to provide the information, the consequences for failure to provide the information, and the individual's access and correction rights. When the information comes from publicly available sources and is used for direct marketing, the individual should be informed, in each communication, of the source of the information, the party responsible for processing, and the individual's data protection rights.

Consent must be freely given, specific, and informed. Unless the law requires explicit consent, tacit consent is valid as a general rule. Where the organization intends to collect personal information directly from the individual, notice must be provided that enables the individual to opt out of processing for purposes that are separate from those that are necessary and give rise to a legal relationship between the individual and the organization. Where personal information is obtained indirectly and there is a change in the purposes that were agreed to in the transfer, the organization must provide the individual with a notice. Where the organization uses remote means or electronic, optical or other technology (e.g., cookies) to collect personal information automatically and simultaneously when the individual contacts them, the individual should be informed at that time about the use of these technologies and how the technology can be disabled.

Express consent is required to process financial or economic data and sensitive information or whenever specified by law or regulation. The organization has the burden of proof to demonstrate that consent was obtained. Consent may be revoked by any means permitted by law.

Right to Digital Oblivion

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. This is one of the first laws to seek to include the right to be forgotten, which has been so controversial in the European Union. 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.

Direct Marketing

Personal information maintained in direct marketing databases may be included only with the consent of the individual or where the information comes from publicly available sources. The individual has the right to access his or her information from such databases free of charge. Electronic marketing communications must offer the right to opt out of future communications or revoke consent. Organizations that maintain such databases must have contracts that provide that the personal information contained in the database has been obtained with the unambiguous and informed consent of the individual or that the information has been obtained from publicly available sources.

Data Security

The organization and, where appropriate, the processor must take the necessary technical and organizational measures to ensure the security of personal information and prevent unauthorized access, use, alternation, disclosure, or transfer. In particular, organizations must develop and implement technical and organizational measures necessary to ensure the integrity, confidentiality and security of the personal information that they process. Such measures must be proportionate to its operations, the risks inherent in these operations, the size of the database, and are subject to the approval of the Directorate which may establish minimum safety standards.

Data Integrity and Data Retention

Personal information that is inaccurate, incomplete, or misleading must be corrected, modified, suppressed, updated or canceled, as appropriate. Personal information should be deleted when it is no longer necessary for the purposes for which it has been processed.

Access and Correction Rights

The individual has the right to request information from the Directorate about the existence of personal data files, their purposes and the identities of those who are responsible for the processing. In addition, the individual has the right to request information directly from an organization that holds files containing his or her personal information. Within 10 working days of receipt of the request, the organization must provide information about how the information was collected, the reasons for the collection, and to whom the information was disclosed. The individual also has the right to amend, modify, delete, supplement, or update his or her personal information; the organization must respond to the correction request within five business days of receipt of the request.

[8] The Law on Personal Data Protection (Act No. 787) of March 21, 2012, is available, in Spanish, at http://legislacion.asamblea.gob.ni/normaweb.nsf/9e314815a08d4a6206257265005d21f9/e5d37e9b4827fc06062579ed0076ce1d?OpenDocument; the Regulation of the Law on Personal Data Protection (Decree No. 36-2012) is available, in Spanish, at http://legislacion.asamblea.gob.ni/normaweb.nsf/9e314815a08d4a6206257265005d21f9/7bf684022fc4a2b406257ab70059d10f?OpenDocument.

  PVLR ISSN 1538-3423

Data Transfers

Personal information may be transferred when the purposes are directly related to the legitimate interests of the organization and the recipient, and the individual is informed about the purposes of the transfer and the identity of the recipient and consents to the transfer. Consent is not required when the transfer is for public health reasons, social interest, national security or where the data have been anonymized. Consent may be revoked by providing a written notice to the organization.

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:

(1) the transfer is for the purposes of international judicial cooperation;

(2) the exchange of personal information is for health matters;

(3) the transfer is necessary to carry out epidemiological investigations, wire transfers or exchanges;

(4) the transfer is required by law;

(5) the transfer is agreed upon under any international treaties ratified by Nicaragua; or

(6) 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, and the request must state the object and purpose of the intended processing. In addition, the organization must comply with the data security and confidentiality measures and verify that the receiving organization complies equally with these measures. The individual must be informed about and consent to the transfer by the organization and the intended purposes of the processing.

Database Registration

Organizations must be registered in the Directorate's database registry and wait 30 days for the Directorate to complete their registration. Organizations must provide their names, addresses, business description, information about the form, time and place of data collection, the purposes of use, intended recipients, the means used to ensure security, the period for which the information will be retained, and the access and correction procedures.

Penalties

Violations of the Nicaraguan Law may result in criminal and/or civil penalties, but no minimum or maximum amounts are specified. The Directorate may also impose administrative sanctions that include warnings, suspension of data processing operations, temporary or permanent closure or termination of databases. The individual may initiate a request for administration action. The Directorate is the only body responsible for hearing and resolving complaints regarding the processing of personal information.

MEXICO

Mexico issued final regulations under the Federal Law on Protection of Personal Data Held by Private Parties in late December 2011.[9] (See our client alert at http://www.mofo.com/files/Uploads/Images/101115-International-Data-Protection-Laws.pdf.) The regulations provide some clarification to the law's notice and consent requirements. It exempts business contact information. The regulations also provide rules specific to cloud computing and allow a data controller to use cloud services where there are contractual conditions for processing and where the service provider meets certain other confidentiality and security requirements.

IMPLICATIONS FOR BUSINESS

With the addition of new laws in Colombia, Costa Rica, Nicaragua, and Peru, there is now a critical mass of countries in the region with privacy regimes that require, among other things, privacy notices and consents, extensive access and correction rights, database registration, and data breach notification. While these laws impose legal obligations common to other privacy laws, particularly those found in Europe, some of the legal provisions, particularly those pertaining to cross-border transfers, are unclear and raise questions about what these requirements mean for organizations in practical terms. Further, unlike the European Union, there is a heavy reliance on consent for cross-border transfers of data. Organizations' compliance efforts are being further challenged by the slow pace at which many of these countries are proceeding to issue implementing regulations and establish data protection authorities. Nonetheless, companies should examine their existing practices and begin to modify their privacy practices in these jurisdictions.

---

[9] The regulations are available, in Spanish, at http://www.profeco.gob.mx/juridico/pdf/r_rpfc_3ago06.pdf (11 PVLR 41, 1/2/12).