Bloomberg BNA

Privacy and Security Law Report®

Data Protection

In this first article in a three-part series on the status of data privacy laws in Latin America, the Caribbean, Asia, Africa and the Middle East, the author explores developments in Latin America and the Caribbean, where several data protection framework laws have been put in place over the past few years.

Privacy in Latin America and the Caribbean

BY CYNTHIA RICH

With the enactment or implementation of several new data privacy laws in the past couple of years, the privacy landscape in Latin America and the Caribbean continues to change dramatically. Twelve countries in the region now have omnibus data privacy legislation in place: Argentina, Bahamas, Chile, Colombia, Costa Rica, Curacao, the Dominican Republic, Mexico, Nicaragua, Peru, Trinidad and Tobago[1] and Uruguay. St. Lucia adopted legislation in 2011, but the law has not yet gone into effect. In addition, other countries such as Brazil or territories such as the Cayman Islands are considering data protection laws.

Unlike the European member state laws that are all based on a common directive, the laws in Latin America and the Caribbean vary significantly from each other. All of these laws are based on 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. For example, unlike the newer laws being adopted in Asia, two-thirds of the new laws in this region require registration with the data protection authority and, in most cases, do not contain detailed security obligations. However, like the new laws in Asia and the existing laws in Europe, many laws in Latin America and the Caribbean impose cross-border restrictions. There is also a growing trend to require notification to regulators and/or individuals in the event of a data security breach. Half of the countries in the region now have such requirements.

Implications for Business

With the addition of new laws in Colombia, Costa Rica, Curacao, the Dominican Republic, 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 consent, 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. A

[1] 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. The act is available at http://www.ttparliament.org/legislations/a2011-13.pdf.

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

 ISSN 1538-3423

careful read of the laws is imperative as they do differ from other established laws and from each other. Further, unlike the European approach, 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. Compliance programs that comply with only EU and Asian obligations will run afoul of many of the Latin American and Caribbean country obligations.

Overview

Before discussing the newest laws in the region (Colombia, Costa Rica, Curacao, the Dominican Republic, Mexico, Nicaragua and Peru), we provide a brief overview of four countries with the oldest or most established privacy regimes in the region (Argentina, the Bahamas, Chile and Uruguay).

Established Privacy Regimes

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.[2] In addition to the usual notice, consent, access and correction requirements, there are detailed security requirements,[3] restrictions on cross-border transfers to countries that do not provide adequate protection and registration requirements. Argentina was the first country 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 (EEA) (2 PVLR 737, 7/7/03).

BAHAMAS

The Data Protection (Privacy of Personal Information) Act 2003 (Bahamas Law) protects personal information of natural persons and applies to the processing of such data by both the public and private sectors.[4] There are broad requirements concerning collection and use of personal information, access and correction rights, data security, retention and destruction and data quality requirements. While there are no explicit notice and consent requirements set forth in the Bahamas Law, the data protection authority (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. There are no registration obligations or cross-border restrictions; however, 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, that need to be met to transfer personal information cross-border.[5]

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.[6] The Chilean Law also contains the usual set of obligations found in most comprehensive privacy laws: notice, consent, access and correction rights, collection and use limitations, security, data retention and data quality. There are no registration requirements and no restrictions on cross-border transfers. Unlike most privacy laws, the Chilean law does not establish a DPA to oversee enforcement of the law.

URUGUAY

Law No. 18.331 on the Protection of Personal Data and Habeas Data Action (Uruguayan Law), enacted in 2008 (7 PVLR 1410, 9/29/08) and amended in 2010, regulates the processing of personal information of natural and legal persons by both the public and private sectors.[7] In addition to the obligations with respect to notice, consent, access and correction rights, data security, data quality and database registration, there are security breach notification requirements and restrictions on cross-border transfers to countries that do not provide adequate protection. Uruguay was the second country in South America to be recognized by the EU as providing an adequate level of protection for personal information transferred from the EU/EEA (11 PVLR 1369, 9/10/12).

New/Recently Enacted Laws

COLOMBIA

Overview

Enacted in October 2012, Law No. 1581, Introducing General Provisions for Personal Data Protection, (Colombian Law) sets forth general rules for the protection of personal information of natural persons by both the public and private sectors, including special protections

[2] The Argentine Law is available, in Spanish, at http://www.infoleg.gov.ar/infolegInternet/anexos/60000-64999/64790/texact.htm.

[3] The security measures are divided into 3 levels: basic- or low-level measures for all databases containing personal data; 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 data.

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

[5] The nonbinding guidance is available at http://www.bahamas.gov.bs/wps/wcm/connect/8931cd1f-90a0-404a-be29-124901e42f61/A+guide+for+Data+Controllers.pdf?MOD=AJPERES.

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

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

  PVLR ISSN 1538-3423

for children (11 PVLR 1573, 10/29/12).[8] The Colombian Law is intended to complement a law enacted in 2008 that applies only to personal credit information. Organizations had six months (until April 17, 2013) to come into compliance with the Colombian Law.

Establishment of 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. It is also 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

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.

Notice and Consent

Organizations must adopt procedures to inform individuals about the personal information to be collected and the purposes of the processing. 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 consent is required to process personal information.

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

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 or 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.

The Superintendence of Industry and Commerce will 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 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. In particular, reasonable steps should be taken to ensure that the information stored in the databases is precise and sufficient and, when requested by the individual or when noted by the organization, the information must be updated, corrected or removed, in order to ensure it meets the purposes of the processing.

Organizations and service providers may only collect, store, use or circulate personal information for as long as is reasonable and necessary for the purposes of the processing and for administrative, accounting, tax, legal and historical purposes. Once the purpose of the processing has been achieved, the organization and the service provider must proceed to remove the personal information in their possession except where such information must be retained in order to comply with a statutory or contractual obligation.

Organizations and service providers must document the procedures for processing, preserving and removing personal data in accordance with the law and instructions from the Superintendence of Industry and Commerce.

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 the purpose of its use. The individual may review his/her personal information at no cost: (i) at least once every calendar month, and (ii) whenever there are substantial changes to the Information Processing Policies. The procedures to access, update, remove and rectify personal information must be disclosed to the individuals or be readily accessible to them and be included in the Information Processing Policy.

The organization or service provider must respond to access requests within 10 business days and correction requests within 15 business days from the date of receipt of the request. This is a very short time period.

Cross-Border Data Transfers

The transfer of personal information to countries outside Colombia that do not provide an adequate level of data protection is prohibited, unless the individual has provided his/her express 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 Colombia is a party, based on the principle of reciprocity;

[8] 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.

- the transfer is necessary in order to execute a contract between the individual and the organization or in order to take pre-contractual 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.

The 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.

Cross-border transfers between an organization and a service provider that are pursuant to a Personal Data Transmission Agreement do not need to be notified to the individual and do not require the individual's consent. Personal Data Transmission Agreements are processing agreements established between the organization and the service providers that establish the scope of the processing, the activities that the service provider will perform on behalf of the organization when processing personal information and the obligations the service provider has toward the individual and the organization. The service provider must be obligated to process the personal information on the organization's behalf, in accordance with the principles that govern that information, safeguard the security of the databases and keep the processing of the personal information confidential.

Database Registration

Organizations and service providers that carry out processing of personal information in Colombia must register with the DPA. A record will be entered into the National Registry of Databases, which is available for public consultation. It is quite unusual to require service providers to file registrations with the DPA.

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.

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 to COP 566,800 (approximately $31 to $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 DPA may order suspension of activities related to the processing of personal information for up to six 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.

COSTA RICA

Overview

Law No. 8968 on the Protection of the Person Concerning the Treatment of Personal Data (Costa Rican Law) came into force Sept. 5, 2011 (10 PVLR 1382, 9/26/11).[9] It applies to automatic and manual processing by both public and private entities. Companies had until March 5, 2013, to bring their practices into compliance with the Costa Rican Law.

Establishment of Data Protection Authority

Prodhab, the data protection authority, established in March 2012, is responsible for creating a database registry, ensuring compliance with the Costa Rican Law and issuing implementing regulations.

Appointment of a Data Protection Officer

There is no requirement to appoint a data protection officer.

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;

(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. Consent can be revoked by the data subject at any time, in the same way it was given. The database controller must establish expeditious, simple and free mechanisms to enable the data subject to revoke his or her consent.

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

- where the processing is 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 or 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 the processing is necessary to establish, exercise or defend individuals' rights in judicial proceedings;

[9] The Costa Rican Law is available, in Spanish, at http://bit.ly/1jwyK5B.

  PVLR ISSN 1538-3423

- 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

Organizations must take any and all necessary precautions to preserve the security and integrity of the information, and to avoid and prevent alteration, damage, destruction, loss and/or any unlawful access and management. Such measures must include, at least, the most appropriate security mechanisms and up-to-date technology to ensure the protection of the information (both physical and electronic). In particular, the organization must establish and maintain administrative, physical and technological measures to protect personal information in accordance with the Costa Rican Law. The organization is responsible for ensuring that its data processor and technological intermediary comply with these security measures.

Organizations will have 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 Integrity and Data Retention

Personal information must be adequate, relevant and not excessive in relation to the purpose of the processing. Personal information must also be accurate and up-to-date for the purpose of the processing.

Organizations must delete or dispose any information when it is no longer necessary for the purpose for which it was stored. In all cases, personal information must not be stored for more than 10 years, unless otherwise required by law or such data are anonymized. The implement regulation characterizes this requirement as ''the right to be forgotten.''

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.

Cross-Border Data 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.

Database Registration

Every database that is established for distribution, promotion or commercialization purposes must be registered with Prodhab; however, the registration procedure is still being developed by the DPA.

Breach Notification

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

Within this same period, organizations should begin a thorough review process to determine the magnitude of the impact, and take the corrective and preventive measures that apply.

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. (The base salary for the year 2013 was defined in the Judicial Bulletin No. 191-2012 of Dec. 13, 2012, as CRC 379,400 (approximately $760)). 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.

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.[10] The Curacao Law is modeled on the Dutch data protection law. The Curacao Law establishes a data protection authority to oversee compliance and imposes restrictions on the cross-border transfer of personal information to countries that do not provide adequate protection; however, there is no requirement to register processing with the DPA.

[10] The Curacao Law is available, in Dutch, at http://www.caribbeancreditbureau.com/index.php/en/legal-privacy/privacy-act-curacao.

DOMINICAN REPUBLIC

Overview

The Organic Law 172-13 on the Protection of Personal Data (Dominican Law), which took effect Dec. 13, 2013, is the most recent law enacted in the region.[11] The Dominican Law protects personal information filed in public or private archives, public records and data banks intended to provide reports. The Dominican Law also regulates credit information companies, the provision of credit reference services and the supply of information on the market to ensure respect for privacy and the rights of the information owners.

The only transition period provided in the Dominican Law pertains to credit information companies, data contributors and financial intermediaries. They have six months from the time this law entered into force to comply with the law.

Establishment of Data Protection Authority

The Dominican Law does not create a DPA; however, the Superintendence of Banks is the entity authorized to regulate credit information companies.

Appointment of a Data Protection Officer

There is no obligation to appoint a data protection officer.

Notice and Consent

Notice must be provided in an express and clear manner when consent of the individual is required to collect personal information. Free, express and conscious consent from the individual is required to process personal information.

Credit Information/Reports. Before requesting and obtaining a credit report, financial intermediaries, economic agents and other individuals or legal entities that have contracted information services from the credit information companies must obtain the individual's express and written consent, indicating in this permission that he/she agrees to allow his/her information to be consulted in the credit information companies' databases.

Consent Exceptions. Consent is not required to process or transfer personal information when:

- the personal information is obtained from publicly accessible sources;
- the personal information is collected in accordance with a legal obligation;
- the processing or transfer pertains to marketing lists, where the information is limited to name, identity and election card, passport, tax identification and other biographical information;
- the personal information is derived from a scientific or professional commercial, employment or contractual relationship with the individual and the processing is necessary for development of that relationship or for compliance purposes;
- the personal information is received from customers in relation to operations conducted by financial intermediaries regulated by the Monetary and Financial Law and economic agents, the credit information companies and entities that develop credit score tools for the evaluation of debtors' risk in the national financial and commercial system;
- the processing or transfer is so provided by a law;
- the processing or transfer concerns personal information in relation to health and is necessary for public health or emergency reasons, or for the conduct of epidemiological studies, as long as the confidentiality of the identity of the individual is maintained via the appropriate mechanisms of disassociation; or
- a procedure of information disassociation has been applied to ensure that the individuals are not identifiable.

In addition, all investigation and intelligent bodies of the state that are in charge of the prevention, persecution and punishment of crimes and offenses are exempt from the consent requirement following authorization from the competent judicial authority.

Processing for Advertising and Market Research Purposes. Personal information may be processed for advertising an market research purposes when it is in documents that are accessible to the public or the information has been provided by the individuals themselves or obtained with their consent. The individual may access the information without any charge and may request, at any time, the withdrawal or blocking of his or her name from these data banks.

Data Security

The organization and, if applicable, the service provider, must adopt and implement technical, organizational and security measures necessary to safeguard any personal information to prevent unauthorized processing, consultation access, alteration or loss. It is prohibited to record personal information in data banks that do not meet technical conditions of integrity and security.

Data Integrity and Data Retention

Personal information that is collected for processing must be true, adequate and relevant in relation to the context and purpose for which it has been obtained. The information must be accurate and updated if necessary. Any information that is wholly or partially inaccurate, or that is incomplete, must be deleted and replaced, or, if applicable, completed by the organization when the inaccuracy or incomplete nature of the information concerned comes to light.

Access and Correction Rights

Individuals have the right to legal action to know about the existence of and to access any information about them that is contained in public or private records or data banks and, in the event of discrimination, inaccuracy or error, to request the suspension, correction and updating of that information.

Cross-Border Data Transfers

Personal information may only be transferred internationally in certain circumstances such as:

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

  PVLR ISSN 1538-3423

- 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; and
- the transfer of legally required information is to safeguard public interest or for the acknowledgement, exercise or defense of a right in a judicial process, or is required by a tax or customs administration to fulfill its duties.

Database Registration

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.

Breach Notification

There is no obligation under the Dominican Law to give notice in the event of a data security breach.

Penalties

Criminal penalties include six months to two years imprisonment and a fine ranging 100-150 current minimum wages. Administrative fines ranging 10-50 current minimum wages are also possible. In addition, there is a private right of action.

MEXICO

Overview

The Federal Law on Protection of Personal Data Held by Private Parties (Mexican Law), enacted in 2010 (9 PVLR 1016, 7/12/10), regulates the processing of personal information of natural persons by private sector organizations but does not apply to duly licensed credit reporting companies.[12] The Mexican Law contains many of the basic obligations that are found in data protection laws around the world but is one of the countries in the region that does not impose registration obligations.

Establishment of 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. It oversees and verifies compliance, issues interpretative guidance and provides technical support to data controllers as requested. The IFAI also issues opinions, recommendations and decisions; disseminates international best practices and standards for information security; and has the power to impose sanctions.

Appointment of a Data Protection Officer or Office

The Mexican Law requires any entity that collects personal information (the data controller or ''organization'') to appoint a data protection officer 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.

Notice

At the time personal information is collected from individuals, the organization must give the individuals a notice that explains what information is being collected and the purposes for which it will be processed. The privacy notice must also, among other things, provide the name and address of the organization collecting the personal information, the choices and means offered to individuals for limiting the use or disclosure of their personal information, the manner in which they may exercise their access and correction rights and, where relevant, notice that cross-border transfers of personal information will occur. If sensitive personal information is to be processed, the privacy notice must state that expressly. Notices must be provided in the same format that is used to collect personal information from the individuals, unless prior notice has been given.

In 2013, the IFAI issued guidelines that provide for three different types of privacy notices: comprehensive, simplified and short.[13] A comprehensive privacy notice must always be made available; however, depending on the circumstances of the data collection, a simplified or short privacy notice may be provided first. The guidelines state expressly that provision of a simplified or short privacy notice does not relieve the organization of its obligation to make available a comprehensive privacy notice.

Simplified or Short Privacy Notice. Where personal information are 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 technology can be disabled by the individual.

Consent

Generally speaking consent is required, but the form of consent varies considerably. Implied consent (or opt-out consent) is sufficient in most instances for the collection, use and disclosure of personal information. If the individual does not object to the processing once he or she has been given the privacy notice, consent will be deemed to have been granted.

Express consent is required to process financial or asset data, and express written consent is required to process sensitive personal information. This written consent can be handwritten, an electronic signature or

[12] The Mexican Law is available at http://www.mofo.com/files/Uploads/Documents/FederalDataProtectionLaw2010.pdf.

[13] The IFAI's guidelines are available, in Spanish, at http://www.mofo.com/files/PrivacyLibrary/temp/MEXICO_Privacy_Notice_Guidelines_Self-Regulatory-Schemes.pdf.

any other authorization mechanism established for the purpose. In general, the form of the consent can be verbal, written, electronic or optical.

If the organization intends to process personal information for another purpose that is not compatible with or analogous to the purposes set out in the privacy notice, new consent from the individual must be obtained.

Data Security

The Mexican Law also requires that the organization establish and maintain physical, technical and administrative security measures to protect personal information from damage, loss, alteration or destruction, or unauthorized use, access or processing. Organizations may not adopt security measures that are inferior to those that they use to manage their own information. The sensitivity of the personal information being collected must be taken into account when adopting these security measures.

The regulations, issued in 2011 (11 PVLR 41, 1/2/12), 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 data; and external inspections or audits to check compliance with privacy policies.[14] 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 data, 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 IFAI may take into account the organization's compliance with IFAI recommendations to determine the attenuation of the corresponding sanction.

Data Integrity and Data Retention

Organizations must ensure that the personal information is relevant, correct and up-to-date for the purposes for which it has been collected.

When personal information is no longer necessary for the fulfillment of the objectives set forth in the privacy notice and applicable law, personal information must be deleted. Information relating to nonperformance of contractual obligations must be deleted after 72 months from the day on which the nonperformance arose.

Access and Correction Rights

Individuals will have the right to access and, where inaccurate or incomplete, correct their personal information. In addition, they will have the right to object to the processing of their personal information, subject to some exceptions. The organization must notify the individual within 20 days from receipt of a request about what actions the data controller will take with respect to the personal information and then must implement the request to correct, delete or update data within 15 additional days.

Cross-Border Data Transfers

If personal information will be transferred to domestic or foreign third parties, the organization must provide the third parties with the privacy notice that was sent to and consented to by the individual. The third parties must process the personal information in accordance with this privacy notice, and assume the same obligations as those assumed by the organization.

In certain cases, domestic or international transfers of data may be carried out without the consent of the individual. For example, personal information may be transferred without consent to affiliated entities that operate under the same internal processes and policies as the organization or under common control of the organization. Consent is also not required where the transfer is necessary to complete a contract between the organization and the third party that is in the interests of the individual, where the transfer is needed for a judicial proceeding or where the transfer is necessary to maintain or fulfill a legal relationship between the data controller and the individual.

Database Registration

There is no database or other registration requirement under the Mexican Law.

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.

Penalties

Violations of the Mexican Law, such as breaching confidentiality, transferring data to third parties without providing the requisite notice or failing to obtain express consent where required, can result in large fines, ranging up to 320,000 days of Mexico City minimum wage (about $1.6 million). Up to 5 years of imprisonment is also possible for crimes relating to the unlawful processing of personal data.

NICARAGUA

Overview

Nicaragua enacted the Law on Personal Data Protection (Act No. 787) March 21, 2012, and the Regulation of the Law on Personal Data Protection (Decree No. 36-2012) (Nicaraguan Law) Oct. 17, 2012.[15] The Nicaraguan Law protects personal information of natural and legal persons in private and public databases.

[14] The regulations are available, in Spanish, at http://inicio.ifai.org.mx/PROTECCIONDEDATOSPERSONALES/RLFPDPP.pdf.

[15] The Nicaraguan Law is available, in Spanish, at http://legislacion.asamblea.gob.ni/normaweb.nsf/9e314815a08d4a6206257265005d21f9/e5d37e9b4827fc06062579ed0076ce1d?OpenDocument; the regulation is available, in Spanish, at http://legislacion.asamblea.gob.ni/normaweb.nsf/9e314815a08d4a6206257265005d21f9/7bf684022fc4a2b406257ab70059d10f?OpenDocument.

  PVLR ISSN 1538-3423

Establishment of a 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 processing of personal information; however, as of April 2014, 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.

Notice and Consent

Prior to processing personal information, notice must be made available to the individual and must 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 Nicaraguan 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 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 EU. 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, alteration, 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 and the size of the database, and they are subject to the approval of the DPA, 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 DPA 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 correction request within five business days of receipt of the request.

Cross-Border Data 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:

(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 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.

Database Registration

Organizations must be registered in the DPA's database registry and wait 30 days for the DPA to complete their registration. Organizations must provide: their name, address and 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. As of April 2014, the registration procedures have not yet been established.

Breach Notification

There is no obligation under Nicaraguan Law to give notice in the event of a data security breach.

Penalties

Violations of the Nicaraguan Law may result in criminal and/or civil penalties, but no minimum or maximum amounts are specified. The DPA 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 administrative action. The DPA is the only body responsible for hearing and resolving complaints regarding the processing of personal information.

PERU

Overview

The Law for Personal Data Protection (Peruvian Law) entered into force July 4, 2011 (10 PVLR 1004, 7/11/11); however, many of the provisions and its regulations did not become effective until May 2013 (12 PVLR 529, 3/25/13).[16] Organizations have until March 2015 to conform their existing personal data banks to the Peruvian Law.

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.

[16] The Peruvian Law is available, in Spanish, at http://www.minjus.gob.pe/wp-content/uploads/2013/04/LEY-29733.pdf.

Establishment of 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.

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 provided by law. To process sensitive information, consent must also be in writing.

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 environments in which the information is processed, stored or transmitted must be equipped with appropriate security controls, based on the recommendations for physical and environmental security contained in current edition of the ''NTP ISO/IEC 17799 EDI Information Technology Code of Good Practices for the Management of Information Security.''

Data Integrity and Data Retention

Personal information that is processed must be accurate and updated. Personal information collected directly from the individual is considered to be accurate.

  PVLR ISSN 1538-3423

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 must adopt a simple procedure to exercise access rights. The exercise of access rights vis-a-vis private-sector personal data banks by individuals must be free of charge, unless otherwise prescribed by regulation. 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.

The organization must respond to the request for information within eight days regarding whether or not it holds the personal information of the individual filing the request. Responses to access requests must be provided within 20 days, and the provision of access must be provided within 10 days thereafter. Where circumstances warrant, the time limits for responding to access requests or provision of access may be extended a single time for a maximum of 20 and 10 days respectively.

If the data were previously transferred, the organization must communicate the updates, amendments, corrections or deletions to the party to whom the information was transferred if the latter continues to process the information. The latter party must also make the changes communicated. During the process of updating, amending, correcting or deleting, the organization must order the blocking of the information and prohibit third parties from accessing the information during this period. The organization must respond to correction, cancellation or opposition requests within 10 working days of receiving the request.

Cross-Border Data Transfers

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

Database Registration

Organizations must register with the DPA. The DPA will review and approve registration applications. Once a personal data bank has been recorded in the National Data Protection Registry, the organization will be notified. If the DPA does not conclude its review and issue a resolution approving, denying or requesting modification of the application within 30 days, the application will be deemed to be accepted and registered, modified or canceled. In addition, organizations that voluntarily adopt codes of conduct to govern their transfers to affiliated entities must register them with the DPA.

Breach Notification

There is no obligation under Peruvian Law to give notice in the event of a data security breach.

Penalties

The 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 to $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.