

MEXICO'S NEW PRIVACY LAW AND REGULATIONS

**By Lic. Carolina Juárez Soler
Guillermo Marrero, Esq.**

Although processing of Personal Data has long been regulated in countries like the United States and the European Union, Mexico has only recently moved forward with regulation of this area. In an effort to catch-up to other countries and meet international standards on the regulation of Personal Data, in July 2010, Mexico passed and published the Federal Law for Protection of Personal Data in Possession of Individuals (*Ley Federal de Protección de Datos Personales en Posesión de los Particulares*) (the "Law"). More recently, on December 21st, 2011, Mexico passed and published the Regulations of the Federal Law for Protection of Personal Data (*Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares*) (the "Regulations"). The purpose of the Law is to regulate the processing of Personal Data by private non-governmental parties.

DEFINITIONS

Personal Data is defined very broadly as any information concerning an identified or identifiable individual.

The Law makes a distinction between Personal Data and Sensitive Personal Data, which is personal data that affects the most intimate sphere of a data subject or which if used improperly may lead to discrimination or entails a serious risk and as a result carries much higher penalties and fines. Sensitive Personal Data may encompass race, ethnic origin, current or future health condition, genetic information, religion, philosophical or moral beliefs, union affiliations, political views and sexual preferences.

Processing means the collection, use, disclosure, transfer or storage of Personal Data.

Transfer means the transmission of Personal Data, inside or outside Mexican territory, to a person other than the data subject, responsible party or department.

PRIVACY NOTICE

Companies and individuals processing Personal Data must provide individual data subjects to whom the Personal Data relates with a Privacy Notice (*Aviso de Privacidad*) advising them of the type of Personal Data and the purpose for which it is being obtained. The Privacy Notice must be prepared in simple terms that are easily understandable and at a minimum must contain:

- Name and contact information of the party processing the Personal Data
- The Personal Data being used
- Purpose for which the Personal Data is being used

- Options available to the data subject to limit use or disclosure of the Personal Data
- Means by which the processor will notify the data subject of the Personal Data of any changes to the Privacy Notice
- Resources available to the data subject to exercise ARCO Rights (as defined below)
- How the data subject may revoke their consent
- Whether Personal Data will be transferred to third parties.

The Privacy Notice may be delivered electronically, via writing or orally.

Although the Law became effective in July 2010, the obligation to provide the Privacy Notice also applies to all processors of Personal Data that obtained Personal Data prior to the Law becoming effective that continue to use the Personal Data.

CONSENT

Subject to the exceptions below, companies generally must obtain the consent of a data subject to process their Personal Data. For Personal Data that is not Sensitive Personal Data or financial data such as income, assets and liabilities, this consent may be implied, meaning that if the data subject does not object to the processing of their Personal Data once a Privacy Notice has been provided to the data subject, then consent is deemed granted. For Sensitive Personal Data, this consent must be express and written, provided by handwritten signature, electronic signature or other means of authentication. For financial data, this consent must be express and may be provided electronically, via writing, visual means, orally or by other certain means. If the purpose for processing Personal Data changes from that set forth in the Privacy Notice, then consent must again be obtained from the data subject. Data subjects may revoke their consent at any time but not retroactively.

Companies do not need to request consent where:

- Use of the Personal Data is for complying with legal relationship obligations (e.g., contract or commercial relationship) between the company and the data subject
- The information is publicly available
- The Personal Data has undergone a process in which Personal Data cannot be associated with the individual or allow identification of the individual
- The processing is permitted or required by law or authority
- An emergency situation exists that could potentially cause damage to the data subject or their property

- Use of Personal Data is necessary to provide emergency health care, diagnosis, medical treatment or sanitary assistance, provided that the data subject is unable to grant consent in accordance with applicable law, including the General Health Law (*Ley General de Salud*) and that processing is executed by a person subject to a confidentiality obligation.

ARCO RIGHTS

The Law and the Regulations set forth a series of rights of data subjects relating to the access, rectification, cancellation and opposition to the use of Personal Data, known as “ARCO Rights”. The Law defines in a broad manner each of these rights. The data subject shall have the right to (1) Access their Personal Data; (2) Rectify erroneous or incomplete Personal Data and processors shall have the obligation of notifying data subjects of any errors or incomplete Personal Data; (3) Cancel the use of Personal Data and (4) Oppose the use of Personal Data at any time.

As of January 6th, 2012, the data subject shall have the right to exercise ARCO Rights directly or through their legal representative by following the procedures set forth in the Privacy Notice. The processor shall have a period of twenty (20) days commencing on the delivery of the request to exercise ARCO Rights to respond to the data subject’s request and a period of fifteen (15) days thereafter to take any necessary actions as a result of the request. The procedures shall at all times be simple and free of charge with the data subject responsible for handling, copying and delivery fees. Failure by the processor to properly respond to a request shall grant the right to the data subject to exercise its rights before the *Instituto Federal de Acceso a la Informacion, “IFAI”*.

The processor must upon notification of a request to cancel Personal Data, block use of Personal Data. This means that the processor may no longer use the Personal Data but may keep a copy in the event that any liability or obligations arise in connection with the relationship between the data subject and the processor and/or the use of the Personal Data. Personal Data retention obligations need to be analyzed on a case by case basis.

PRIVACY DEPARTMENT

Processors must designate a person or department that is responsible for responding to requests or inquiries and request to exercise ARCO Rights from data subjects. In addition, the responsible party or department shall be responsible for implementing safety measures to prevent unauthorized access to the Personal Data and damage to the equipment or location where the Personal Data is maintained and guaranteeing safe disposal of Personal Data.

TRANSFERS

Subject to the exceptions below, a data subject must consent to any transfer of Personal Data to a third party that is not a service provider and such transfer generally must be reflected in the Privacy Notice. A company needs to provide the Privacy Notice to such third party and

take steps to ensure that they comply with the Law and with the Privacy Notice, including through written contract. Exceptions to the consent requirement include transfers:

- To an affiliate or subsidiary of the company
- That are necessary because of an agreement for the benefit of the data subject, by the company and the third party
- That are necessary to comply with a legal relationship between the company and the data subject
- That are made relating to legal proceedings, investigations or required by law or authority.

A company must take steps to ensure that service providers to which Personal Data is transferred comply with the Law and with an applicable Privacy Notice, including through written contract. The burden of proof on compliance shall be on the Processor and the third party.

DATA BREACH

Processors shall establish and maintain administrative, technical and physical safety measures to ensure protection of Personal Data against damage, loss, alteration, destruction, access and unauthorized use. When determining the safety measures to be implemented, the processor should consider the potential risks, consequences to the data subjects in the event of a Data Breach (as defined below) and whether Personal Data is Sensitive Personal Data. Safety measures shall be at minimum equal to those used by the processor in the protection of their own data.

Data Breach includes:

- Unauthorized loss or destruction
- Theft or unauthorized copying
- Unauthorized processing or access
- Damage, alteration or unauthorized modification.

Immediately after the occurrence of a Data Breach and after taking all necessary steps to assess the nature and extent of the Data Breach, the processor shall notify the data subject of: (1) nature of the Data Breach; (2) Personal Data compromised; (3) recommendations to protect the Personal Data; (4) actions taken to correct the Data Breach; and (5) means through which the data subject may obtain additional information concerning the Data Breach. After a Data Breach, the processor is required to analyze the causes of the Data Breach and to take corrective measures to prevent it.

COMPLIANCE, ENFORCEMENT AND PENALTIES

The *Instituto Federal de Acceso a la Informacion*, “IFAI” is the governmental entity responsible for: (1) overseeing enforcement of the provisions of the Law and its Regulations; (2) responding to complaints filed by data subjects against processors and (3) imposing sanctions for non-compliance. The IFAI is vested with inspection rights and has the power to verify compliance by processors.

Data subjects may directly or through their legal representatives initiate a procedure before IFAI, known as Procedure for the Protection of Rights against processors arising from actions or omissions in connection with the exercise of ARCO Rights. Data subjects shall have the right to initiate this procedure when processors:

- Fail to respond to a request to exercise ARCO Rights
- Deny access to the Personal Data
- Deny changes to Personal Data
- Provide insufficient or incomplete information
- Deny cancellation of Personal Data
- Continue to use Personal Data regardless of a request to oppose use
- Other causes that the IFAI considers applicable in accordance with the Law and the Regulations.

Parties found to be non compliant may be sanctioned with monetary sanctions ranging from 100 to 160,000 times the minimum wage in Mexico D.F.¹ (approximately US\$450 to US\$725,000) in cases of negligent or malicious use of Personal Data, omissions in the Privacy Notice, and sanctions ranging from 200 to 320,000 times the minimum wage in Mexico D.F. (approximately US\$907 – US\$1,450,000) for substantially changing the purpose for which the Personal Data is collected, unauthorized transfer of Personal Data to third parties, fraudulent acquisition of Personal Data, among others.

In addition to monetary sanctions, criminal charges may be imposed against parties found liable. Such crimes may be punishable by prison time of 3 months to 6 years to processors who with intent to profit breach the security of a database under their supervision and 6 months to 5 years to those who with intent to profit acquire Personal Data through fraud.

Processors shall have the right to oppose any adverse resolutions issued by IFAI in Procedure for the Protection of Rights and the application of sanctions and penalties through a Nullity Trial (*Juicio de Nulidad*) before the *Tribunal Federal de Justicia Fiscal y Administrativa*.

RECOMMENDATIONS

¹ Minimum Wage in Mexico D.F. is \$62.33 Pesos

Companies and individuals conducting businesses in Mexico should review their existing policies and practices in light of the Law and Regulations and assess compliance. At a minimum they should:

- Prepare a Privacy Notice and provide to data subjects
- Obtain consents from data subjects where needed
- Designate an individual or department to respond to ARCO Rights requests
- Ensure compliance with the Law and applicable Privacy Notices in the case of transfers
- Establish and maintain adequate safety measures to prevent Data Breaches
- Establish procedures on how to respond and resolve Data Breaches
- Train personnel and employees who will handle Personal Data.

For more information, please visit us at www.ipglaw.com

International Practice Group P.C. is a boutique law firm specialized in cross border matters. IPG has a unique practice with a unique combination of attorneys from both Mexico and the U.S. offering legal services in both countries with the ability to represent clients in English and Spanish. IPG's practice and experience includes: Litigation, Corporate, Real Estate and Cross Border Transactions (U.S.-Mexico). Mr. Marrero is a Partner at IPG with over 30 years of experience. Mr. Marrero's practice focuses in structuring and implementing cross border commercial ventures, international joint ventures and the representation of companies seeking to do business in or with Mexico and other Latin American countries. Mr. Marrero also devotes a significant percentage of his practice handling civil litigation matters both domestic and international. Ms. Juarez is an Associate at IPG and a licensed Mexican attorney. Ms. Juarez practice at IPG focuses on international business transactions with an emphasis on U.S.-Mexico cross border transactions, corporate and real estate matters.

Guillermo Marrero
International Practice Group
1350 Columbia St., Suite 500
San Diego, CA 92101
Direct: (619) 515-1482
gmarrero@ipglaw.com
www.ipglaw.com

Lic. Carolina Juárez Soler
International Practice Group, P.C.
1350 Columbia, Street, Suite 500
San Diego, CA 92101
Direct: (619) 515-1487
cjuarez@ipglaw.com
www.ipglaw.com