

## ALERTS AND UPDATES

### Privacy Notice to Be Given by Mexican Entities and Individuals Under the Federal Protection Law of Personal Data

June 28, 2011

#### 1. Description of Mexico's Federal Protection Law of Personal Data

The Federal Protection Law of Personal Data (the "Law") was published in the [\*Mexican Federal Official Gazette\*](#) on July 5, 2010, in Mexico City and was effective one day after its publication. This Law regulates the manner and conditions in which personal data can be used by entities and individuals that obtain personal data from individuals. Its purpose is to guarantee the protection of personal information and the individuals' right to decide on how individuals and entities use their data. Pursuant to the transitory articles of the Law, the regulations of the same will be published no later than July 6, 2011.

The Law provides that when handling personal data, there is a reasonable expectation of privacy; and when an individual or entity responsible for the handling of data obtains personal data or sensible personal data, the individual or entity is required to obtain the express consent of the holder of the data.

The Law defines personal data as any information concerning an individual identified or identifiable and defines as sensitive personal data the personal data that affects the most-intimate sphere of the holder or which unlawful use could cause discrimination or convey a gross risk to them. In particular, it encompasses data that can reveal aspects like racial or ethnic origin; actual and future health; genetic information; religious, philosophical and moral beliefs; labor union affiliation; political opinions; and sexual preference.

#### 2. Privacy Notice—Immediate Action to Be Taken

Notwithstanding that the Law exempts certain individuals and entities—that the Law defines as responsible—from requesting consent from the holders of the data when a legal relationship between the entity and the holder of the data exists, the Law obliges the individuals and entities to give a privacy notice. This notice is a document in hard-copy or electronic format made available, through physical, digital, visual or sound means or any other technology, to the holder of the data (the "Privacy Notice"). Pursuant to the Law, individuals and entities in receipt of personal data are required to provide such Privacy Notice to the holders of the data no later than **July 6, 2011**. In addition, any changes or modifications to such Privacy Notice must be conveyed to the holder of the data. The Privacy Notice applies to Mexican employers who possess data of employees and which are required under the Law to provide the Privacy Notice to their employees.

The following are the minimum requirements the Privacy Notice has to contain:

- Identity and domicile of the responsible individual or entity;
- Purpose of the data use;
- Options and methods to limit the use and disclosure of the data;
- Means or mechanisms to exercise the rights of access, correction, cancelation and opposition;
- The transfer of data that will be made; and

- The mechanism or proceeding by which the responsible individual or entity will inform the holders of any changes to the Privacy Notice.

In the event that the individual or entity in receipt of personal information makes any transfer of data, it is unnecessary to indicate such transfer in the privacy notice if:

- The transfer is foreseen or established in a law or treaty to which Mexico is a party;
- The transfer is necessary for medical attention, prevention, diagnosis, rendering of sanitary assistance, medical treatment or execution of sanitary services;
- It is done between related parties;
- It is necessary by virtue of an agreement executed or to be executed between the responsible individual or entity and a third party at the interest of the holder;
- It is necessary or legally claimable for the safeguard of a public interest, or for the provision and administration of justice;
- It is necessary for the recognition, exercise or defense of any right in a judicial process; or
- It is necessary for the maintenance or fulfillment of a legal relationship between the individual or entity responsible for the data and the holder.

### **3. Main Responsibilities of the Entities or Individuals Handling the Data**

- Designate a responsible individual in charge of handling and correcting the personal data, and develop the processes for consulting or correcting the information. This designation has to be made no later than July 6, 2011.
- Obtain the consent of the holder of the data (except in the specific cases provided by the Law) if the purpose of usage of the data changes.
- Issue the Privacy Notice and verify its fulfillment and authorization. This notice has to be given no later than July 6, 2011.
- Include in the Privacy Notice the consent of the holder of the data to transfer data (except in the specific cases provided by the Law).
- Establish the handling that will be given to personal data.
- If databases are created, they have to contain minimum information in accordance with the purpose of their use.
- Maintain confidentiality of the information (continues after the legal relationship has been finished) and extends to third parties.
- Provide personnel training (such as a handbook of practices or process guidelines).
- Establish proceedings for the holder to exercise his rights.
- Establish safety measures for the handling of the data to avert modification, loss and unauthorized access.
- Comply with the time frames to respond to requests and implement the requested changes (20 days and 15 days, respectively).

#### **4. Breach of the Law**

Each of the following events constitutes a breach of the Law:

- Failure to fulfill the request made by the holder to exercise the rights of access, correction, cancelation and opposition to the handling of their personal data, without a justified reason.
- Act with negligence or bad faith in the process or response of the holder's requests.
- Declare with bad faith the inexistence of data, when there is actually data or part of the data in the responsible party's databases.
- Handle the data contravening the Law.
- Failure to include in the Privacy Notice all the items mentioned in article 16 of the Law that are described in section three above.
- Keep data that are incorrect or imprecise, or failure to make the corrections or cancellations of the data according to the Law.
- Failure to comply with the disciplinary measure of the authorities in order to perform what the holder of the data requested.
- Failure to comply with the confidentiality duty.
- Substantially change the original purpose of the handling of the data, without obtaining a new consent of the holder.
- Transfer data to third parties without informing them of the Privacy Notice.
- Affect the safety of the local databases, programs or equipment.
- Perform the transfer of data in the cases not allowed by the Law.
- Obtain or transfer personal data without the express consent of the holder.
- Obstruct or hamper the verification acts of the authority.
- Obtain data in a deceitful or fraudulent manner.
- Continue with the illegitimate use of the data when the cease of their use was previously requested.
- Handle the data impeding or affecting the exercise of the holder's rights.
- Create databases with a purpose other than for the one they were created.
- Any breach by any individual appointed by the entity as responsible for the data.

#### **5. Sanctions**

Sanctions vary from a disciplinary measure against the responsible party in breach of the Law to a fine from 100 to 320,000 days of the minimum general wage effective in the federal district, and additional fines in the case of relapse.

It is a crime if the responsible individual or entity handles the data with the purpose of obtaining a profit that would render vulnerable the safety of the databases. This conduct would result in a sentencing of three months to three years in prison. If the responsible individual or entity takes advantage of the error and obtains data by means of fraud or deception, the sanction is six months to five years in prison; and if it is related to sensible data, the sanctions are doubled.

## **About Duane Morris and Miranda & Estavillo**

International law firm Duane Morris LLP and Mexico City law firm [Miranda & Estavillo, S.C.](#) have entered into an agreement creating an alliance that formalizes and strengthens a longtime referral and networking relationship between the two firms. The firms have provided clients with legal counsel on U.S. and Mexican legal issues, particularly in the area of international corporate transactions. The firms will now offer clients expanded geographic reach and practice strength in cross-border matters.

### **For Further Information**

If you would like additional information regarding Mexico's federal law on protecting personal data, please contact any of the [members](#) of the [Mexico Business Group](#) or the attorney in the firm with whom you are regularly in contact.

*Disclaimer: The alliance between Duane Morris and Mexico City law firm Miranda & Estavillo, S.C. is based on a cooperative relationship agreement. Clients of one firm are not clients of the other unless an explicit agreement has been executed that confirms that an attorney-client relationship has been established and the terms of that relationship.*

*Disclaimer: This Alert has been prepared and published for informational purposes only and is not offered, or should be construed, as legal advice. For more information, please see the firm's [full disclaimer](#).*