A Timely Analysis of Legal Developments

ASAP®

April 5, 2013

Mexico's New Privacy Notice Guidelines Require Immediate Action

By Javiera Medina Reza and Eduardo Osornio Garcia

On April 17, 2013, Mexico's new Privacy Notice Guidelines will go into effect. The Guidelines impose extensive requirements for furnishing adequate data privacy notices and obtaining consent before personal data is collected directly from a person or electronically via "cookies," "web beacons" or other automated means. The Guidelines are mandatory and particularly important to employers that regularly collect, process, and/or transfer personal data about employees or job applicants, and to companies operating or advertising in Mexico that use cookies, web beacons, and similar media technology that automatically collects personal data online. As shown in a recent decision by the Federal Institute for Access to Information and Data Protection ("IFAI" for "Instituto Federal de Acceso a la Información y Protección de Datos"), sanctions may be imposed for noncompliance.

Privacy Law

On July 5, 2010, Mexico enacted a comprehensive collection of data privacy laws known as the Federal Law on the Protection of Personal Data Held by Private Parties ("Ley Federal de Protección de Datos Personales en Posesión de los Particulares") ("Privacy Law"). The Privacy Law provides that all individuals have an inviolate federal constitutional right to the protection of their personal data, as well as a right to access, correct, cancel and challenge the use of such information. These privacy rights are a constitutional cornerstone found in Article 16 of Mexico's Magna Carta.

The IFAI is empowered to guarantee the protection of all personal data and prosecute any violations of the Privacy Law. Its Guidelines interpret the Privacy Law with regards to the treatment of personal data, the content required for a privacy notice, and how it can be delivered.

Privacy Notice and Consent Requirements

The Guidelines impose various obligations on "data controllers" and "data processors." The Privacy Law defines a *data controller* as the individual or legal entity that decides how personal data is processed, and a *data processor* as the individual or legal entity that, alone or jointly with others, processes personal data on the data controller's behalf. A *data owner* is the individual to whom the personal data relates. In many cases, the data controller or processor may be an employer or an employer's agent, and the data owner may be an applicant or employee.

The Guidelines establish that before the "responsible party," or the party handling an individual's personal data (including data controllers and data processors), can collect, process, or transfer personal data, the data owner must receive a privacy notice and be afforded the opportunity to consent to his or her personal data being processed. If the responsible party collects personal data automatically through electronic means (*e.g.*, using cookies or web beacons to track website visitors), the responsible party must provide the user a privacy notice and the opportunity to disable cookies or web beacons to prevent data collection, unless such technology is necessary for the electronic platform to properly function.

The privacy notice is provided by the responsible party to the data owner, through print, digital, visual or audio formats or any other technology, and informs the data owner that his or her data will be collected, how such data will be processed, and the purpose for such processing. The responsible party may issue the notice in a "full," "simplified," or "short" form, depending on how the personal data will be collected.

Full Notice

When the responsible party collects personal data directly from the data owner (*e.g.*, when an individual provides personal data in a job application), it must provide a full notice and obtain the data owner's consent. A full notice must contain the following information:

- Notice that the data owner's consent is required before personal data can be collected, processed, or transferred, which provides the data owner the opportunity to consent to or reject the data treatment;
- The type of data being collected;
- The responsible party's identity and address (including the full name of the individual and the corporate name of the legal entity, where applicable);
- The purpose or actions driving the data collection or processing;
- The mechanisms through which the data owner can exercise his or her right to access, rectify, cancel, or object to how personal data will be used or processed (known as "ARCO" rights), or to revoke consent;
- The means to limit the use, disclosure, or transfer of the data, including notice of and the opportunity to disable cookies and/or web beacons before personal data is automatically collected; and
- The method by which the responsible party will inform the data owner of any changes to the privacy notice.

Simplified Notice

When the responsible party collects personal data directly or indirectly from the data owner, a simplified notice must be provided that includes:

- The responsible party's identity and address;
- Why the data is being collected;
- How to limit data use or disclosure;
- How to exercise ARCO rights; and
- How to access the full notice.

Short Notice

The responsible party may provide a short notice when the space to transmit the privacy notice is limited. The notice must include:

- The responsible party's identity and address;
- Why the data is being collected; and
- How to access the full notice.

To ensure its efficacy, the privacy notice must be written in Spanish in simple, clear, and understandable language, in a structure and design that facilitates its understanding. It must not use inaccurate, ambiguous or vague phrases, or language or formatting that will induce the owner to choose one specific option over another.

Recommendations in the Guidelines

An addendum to the Guidelines provides several recommendations for best practices, some of which are mentioned here. First, when personal data is collected from a person known to be underage or legally incompetent, the privacy notice should explain how a legal custodian can provide consent to data collection, as required under the Federal Civil Code. The responsible party should also implement mechanisms to protect the privacy rights of this vulnerable group of individuals. Additionally, the privacy notice should inform the data owners that they can contact the IFAI in the event that the personal data has been compromised.

Entities handling personal data are also encouraged to implement frameworks and policies to measure how effectively they protect personal data. In June 2013, the IFAI is expected to promulgate new guidelines establishing frameworks to assist entities with implementing binding self-regulation.

Recent Enforcement Activity

A recent decision by the IFAI illustrates the importance of fully complying with the new Guidelines. In December 2012, the IFAI found that Farmacias San Pablo, a company based in Mexico, violated the Privacy Law when it required that patients' names and addresses be included on all prescriptions for psychotropic medications, but failed to provide a privacy notice informing the public about how personal data would be used and treated. Further, the IFAI found that the company's privacy notice was deficient because it failed to provide the name and address of the party collecting personal data. The company failed to cure the irregularities and the IFAI imposed over two million Mexican pesos (over $162,000 USD) in sanctions against the company's parent company, Pharma Plus S.A. de C.V.

As the Farmacias San Pablo case demonstrates, the Mexican government is now actively monitoring whether companies are complying with the law, and prosecuting and penalizing noncompliant entities.

Final Considerations

The requirement to furnish a privacy notice came into effect with the enactment of the Privacy Law in July 2010. The Guidelines, which become effective April 17, 2013, illuminate this requirement's contours and reinforce the need to ensure that data protection policies are fully compliant. No company is "grandfathered" in or otherwise exempted from compliance. Accordingly, companies operating in Mexico should be prepared to provide the privacy notice to current and prospective employees if they process these individuals' personal data.

Companies operating in Mexico should immediately implement internal processes for the proper collection, use, storage, and transfer of personal data, especially if the data will be transferred from their database to a third party, such as when employers transfer employees' personal data to an insurance carrier or from one affiliate to another, or work with third parties to conduct background checks of job applicants. It is equally important to ensure that services agreements include specific provisions setting forth the parties' obligations concerning protection of personal data.

Javiera Medina Reza is a Shareholder, and Eduardo Osornio Garcia is a law clerk, in Littler, De la Vega y Conde's Mexico City office. If you would like further information, please contact your Littler attorney at 1.888.Littler or info@littler.com, 52.55.5955.4500 (Mexico City), 52.81.8851.1200 (Monterrey), Ms. Medina Reza at jmedina@Littler.com, or Mr. Osornio at eosornio@littler.com.