JULY 2010

NEW MEXICAN DATA PROTECTION LAW: STRICT REQUIREMENTS AND SEVERE PENALTIES

Mexico's Department of the Interior has announced that the country's new Federal Law for Protection of Personal Data held by Private Persons (*Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, "LFPDP" or the "Act")[1] came into effect on July 6, 2010. The Mexican Senate unanimously voted to pass the Act, which was nearly 10 years in the making. The Act aims to protect personal data relating to Mexican citizens held by individuals and private entities.[2]

The Act's intent is to enforce "controlled and informed" processing of personal data in order to ensure that Mexican citizens, referred to as "data subjects", possess "privacy and right to self-determination." Data subjects ultimately decide how their personal data will be used, *i.e.*, it must be used solely for the purpose for which it was provided and according to the terms outlined in the privacy notice. Companies handling information about Mexican citizens will be forced to comply with specific obligations in the processing of personal data or suffer severe penalties.

The Act requires companies to inform data subjects about the information being used and the purpose for such use via a privacy notice. It also provides special requirements for processing "sensitive personal data." The Act gives data subjects the right to:

- access their data;
- have inaccuracies in their data corrected;
- deny transfers of their data; and
- oppose use of their data or have it deleted from a company's system for "legitimate"[3] reasons.[4]

While the Act does not provide a comprehensive data breach notification provision similar to U.S. state laws, it requires "immediate" notice to a data subject of any security breach that "significantly" affects his/her "property or moral rights."[5]

With the passage of the Act, the Federal Institute of Access to Public Information changes its name to Federal Institute of Access to Information and Data Protection[6] (the "Institute"). The Institute is authorized to monitor and enforce compliance with the Act by private companies processing personal data.[7] Companies will be held liable for interfering with a data subject's exercise of his/her rights under the Act and for failing to safeguard his/her personal data. Data subjects who believe that a company is not processing their personal data in accordance with the Act may also request an investigation by the Institute.[8] Following an investigation, the Institute may dismiss the data subject's claim or affirm, reject, or modify a company's answer to a data subject's claim.[9]

The Institute's decision may be appealed before the Federal Tribunal of Fiscal and Administrative Justice (the "Tribunal") by either the data subject or the company processing the personal data.[10] Penalties for violating the Act's provisions can be as severe as a US$1.4 million fine, a prison sentence of five years, or double the penalties in the event of sensitive personal data.[11] Below is a summary of a company's obligations under the Act and a description of possible penalties for failure to comply with its provisions.

OBLIGATIONS UNDER THE ACT–A COMPANY'S PERSPECTIVE

Covered Entities and Application

The Act creates obligations for "natural persons or private legal entities that process personal data" concerning Mexican citizens.[12] The Act does not apply to certain companies in the credit information business or to the use of personal data that is personal; that is, use of personal data that is not for disclosure or commercial purposes.[13] Thus, in general, the Act imposes restrictions and obligations in the "processing" of "personal data," with more onerous restrictions and obligations on the processing of "personal data" relating to Mexican citizens. Such restrictions also apply on the transfer of such personal data outside of Mexico.

The Act defines "processing"[14] as the "collection, use, disclosure or storage of personal data by any means," including "any act of access, management, use, transfer or disposal of personal data."[15] "Personal data" is also defined broadly and means "any information concerning an identified or identifiable physical person."[16] "Sensitive personal data" is defined as "personal data involving the most intimate sphere of the data subject, or whose misuse can lead to discrimination or cause a serious risk to the data subject."[17] Sensitive personal data includes data containing information about race, ethnicity, health status, genetic information, religion, philosophical or moral beliefs, union membership, political views, or sexual preference.[18]

Principles for the Protection of Personal Data

Notice and Consent. The Act provides that there is a "reasonable expectation of privacy" in the processing of personal data and requires consent by the data subject prior to such processing.[19] Generally, according to the Act, consent can be obtained by means of a privacy notice that informs the data subject of the information being used, the method of use, the purpose for such use, and the data subject's rights of "access, rectification, and cancellation or opposition."[20] Under the Act, data subjects may revoke consent at any time without retroactive effect, and companies must establish and explain procedures for such revocation within their privacy notice.[21]

Processing of sensitive personal data requires written consent from the data subject via a handwritten signature, electronic signature, or authentication mechanism.[22] The privacy notice must expressly state that the data to be used is of a sensitive nature.[23] Moreover, the Act prohibits the creation of databases containing sensitive personal data without "legitimate" business justification.[24] Where extenuating circumstances would make it "impossible" to provide a privacy notice, a company may, with the authorization of the Institute, implement alternative methods for providing such notice.[25] It is not known at this time what form such alternative methods might take, but companies operating in Mexico might anticipate that such methods will be aimed at accomplishing the same legal principles and objectives of the Act, and thus could be onerous.

Privacy Notice Content. Under the Act, a company's privacy notice must, at a minimum, inform data subjects about:

- the company's identity and address;
- the purpose for processing the data;
- the options and means available to the data subject for limiting use or disclosure of his/her personal data;
- the means by which the data subject may exercise his/her rights of access, rectification, cancellation, and opposition under the Act;
- any planned transfer of the data; and
- the procedure and means for informing the data subject about changes to the privacy notice.[26]

If a company plans to process sensitive personal data, its privacy notice must expressly state that it is doing so.[27]

Accuracy of Data and Purpose of Use. The Act requires companies to ensure that personal data is accurate and up-to-date.[28] It also requires a company to dispose of the data once it has served the original purpose outlined in the privacy notice.[29] A company must make "reasonable efforts" to finish its processing of sensitive personal data as quickly as possible.[30] However, the Act does not define what is meant by "reasonable efforts." Accordingly, companies might, at a minimum, consider adopting established industry practices, and implementing internal policies, that define temporal limitations on the processing of sensitive data, including its destruction, to address this requirement.

If a company intends to use the personal data for any purpose not outlined in the privacy notice, it is required to provide notice and obtain renewed consent from the data subject.[31] Any personal data retained for the purpose of proving or disproving a claim of breach of contract must be eliminated after 72 months from the date of the alleged breach.[32]

Responsibility for Third-Party Use. The Act also addresses certain responsibilities in relation to third parties. Companies are required to adopt "necessary" measures to ensure compliance with the Act, including by third parties.[33] This obligation exists even if the company employs a third party to assist in the processing of the personal data.[34] A company must take "necessary and sufficient" measures to guarantee that the terms of the privacy notice are respected at all times by the company and by any third parties with which it bears "some legal relationship."[35] Thus, the Act requires that companies legally impose on their third-party providers and partners necessary and sufficient binding obligations consistent with the Act's requirements and the company's privacy notice. This has often been done in the form of a binding data processing and protection agreement between the company (*i.e.*, the data controller that collects and/or is in possession of the personal data) and the third-party data processor.

Security Measures in Maintaining Data. The Act requires companies to establish and maintain security measures and administrative techniques to protect the personal data against damage, loss, alteration, destruction, or unauthorized access or use.[36] While the Act does not specify the types of security measures that a company must implement, it requires that such measures be at least as comprehensive as those used to protect the company's proprietary information.[37]

Data Breach Notification. The Act requires "immediate" notice to the data subject of any security breach that "significantly" affects his or her "property or moral rights."[38] The Act, however, does not provide guidance on what is meant by "immediate" or the form and substance of such notices. It is also not known whether the term "significantly" is meant to impose some "risk of harm" threshold or condition prior to providing notice. It is possible, and indeed likely, that the Institute may provide guidance on how companies may meet these requirements. Until then, companies may look to recent experiences in other jurisdictions where similar data breach notifications are required.

Confidentiality. The Act requires companies and third parties involved in the processing of personal data to maintain the confidentiality of personal data at all times.[39] The obligation to maintain confidentiality exists even after the relationship with the data subject ends.[40]

Data Subject Rights

Data subjects generally have the right to oppose use of their data, access their data, have inaccuracies in their data corrected, or have their data deleted.[41] A data subject's request for cancellation triggers a "blockade period" during which the personal data shall be suppressed.[42] During this period, a company may only retain the personal data for purposes of investigating liability arising from such use.[43] This "blockade period" is equal to the statute of limitations time for actions arising from the relationship between the parties.[44]

The Act requires a company to appoint a specific person or department to address requests by data subjects asserting the rights listed in the preceding paragraph.[45] After receiving the request, a company has 20 days to contact the data subject.[46] A company must state its determination in its response and implement the communicated plan of action, if any, within 15 days from the date of the response.[47] One extension of these time limits is available if warranted by the circumstances.[48]

A company's requirement to provide access to the personal data is satisfied when the data is available to a data subject either through simple copies, electronic documents, or any other form set forth in the company's privacy notice.[49] A company cannot charge a data subject for access to his or her personal data, with the exception of "justified" shipping and reproduction costs.[50] However, a data subject may be charged up to approximately US$13[51] for a repeat request within a 12-month period, unless the repeat request is prompted by a substantial change to the privacy notice.[52]

If a data subject requests rectification or cancellation of his or her personal data, a company must also notify third parties to which it transferred the data.[53] If removal is required, a company must notify the data subject once his or her personal data is removed from the system.[54]

Data Transfers

In most instances, a company must disclose to data subjects any planned transfer of personal data to third parties and include a clause in the privacy notice allowing the data subject to accept or deny such transfer.[55] Once personal data is transferred to a third party, that third party is also subject to the requirements of the Act.[56] The Act provides that national or international transfers of data may be carried out without the consent of a data subject when the transfer is made to, among others, holding companies, subsidiaries or affiliates under common control of the company, or a parent company or any associated company working under the same processes and internal policies.[57]

Procedure for Data Subject Exercise of Rights

In some cases, a data subject may petition the Institute to ensure that a company satisfies its duty to the data subject under the Act.[58] The data subject must submit this petition within 15 days from the date that the company responds to its opposition or request for access, rectification, or deletion of data.[59] The Institute will conduct its own investigation and make a determination as to whether or not the company has satisfied its duty to the data subject.[60] If the Institute determines that the company has not satisfied its duty, the company must comply with the Institute's decision and provide the Institute with a written account of its compliance within 10 days of being notified of the decision.[61] The Institute's decisions may be appealed to a tribunal for adjudication.[62]

Procedure for Verifying Compliance

The Institute is authorized to check whether a company is in compliance with the Act.[63] This verification may be initiated at the Institute's discretion or at the request of a data subject.[64] During the verification process, a company is required to provide the Institute with access to the information and documentation that the Institute deems necessary and relevant to its investigation.[65]

VIOLATIONS AND PENALTIES

In penalizing a company for violating the Act, the Institute considers: the nature of the data involved; whether there was blatant impropriety on behalf of a company in responding to a data subject's request; whether a company's act or omission was intentional; a company's financial capacity; and whether a company has previously violated the Act.[66] Penalties for violations of the Act may include:

1) Warning: A warning issued to comply with a data subject's request for access, rectification, cancellation, or opposition pursuant to the Act.[67]

2) Fine:

a) A fine up to about US$736,300 for any of the following violations:[68]

- Acting with negligence or willful misconduct in processing data and responding to a data subject's requests for access, rectification, cancellation, or opposition.
- Fraudulently declaring that the company does not have the personal data when such data exists at least partially in the company's database.
- Processing personal data in a manner conflicting with the principles of the Act.
- Omitting any required elements from the privacy notice.
- Failing to maintain accurate data or failing to implement rectifications or cancellations lawfully requested by a data subject.
- Failing to comply with the Institute's warning to grant a lawful request by a data subject pursuant to the Act.

b) A fine of up to about US$1.4 million for any of the following violations:[69]

- Failing to maintain the confidentiality of information obtained through processing of the data.
- Substantially deviating from the purpose of use originally outlined in the privacy notice.
- Transferring personal data to third parties without first disclosing the planned transfer and providing the data subject an opportunity to opt out of such use in the privacy notice.
- Creating vulnerabilities in the security of the database, facilities, programs, or equipment used in processing the personal data.
- Transferring or assigning personal data except where allowed by the Act.
- Collecting or transferring personal data without the express consent of the data subject where such consent is required by the Act.
- Obstructing investigations by the authorities.
- Collecting data through deceptive or fraudulent means.
- Continuing prohibited use of personal data after being asked to cease such use by the Institute or the data subject.
- Processing personal data in a way that affects or impedes the data subject's right to access, rectification, cancellation, or opposition.
- Creating a database containing "sensitive personal data" without a legitimate purpose.

c) An additional fine of up to about US$1.4 million for continuing violations.[70]

d) Double the applicable fine for violations involving "sensitive personal data."[71]

3) Imprisonment:

a) Three months to three years of imprisonment for anyone authorized to process personal data who, for profit, causes a security breach to the database under his charge.[72]

b) Six months to five years of imprisonment for anyone who, in taking advantage of an error committed by the data subject or person authorized to transmit the data, deceptively processes personal data with the goal of obtaining unjust profit.[73]

c) Double the applicable prison term for cases dealing with "sensitive personal data."[74]

CONCLUSION

The Act aims to safeguard individuals' autonomy in the use of their personal information and to prevent such information from being compromised. With overwhelming support from the Mexican government, the Act has now become law and creates strict requirements for companies processing individuals' personal data relating to Mexican citizens. To avoid severe penalties, companies should draft comprehensive privacy policies, procedures, and guidelines aimed at satisfying the new legal requirements under the Act. Such policies and procedures should address the managerial, operational, and technical measures the company employs to satisfy the notice and consent requirements, and that provide data subjects an opportunity to opt out of third-party transfers.

Companies should also develop internal mechanisms to ensure that personal data is protected, accurate, and used within the confines of the privacy notice. It is common, and indeed now mandatory, that companies establish specific procedures and appoint dedicated personnel to respond to data subject requests as efficiently as possible and in accordance with obligations under the Act. Legal counsel can offer advice and guidance on establishing or revising privacy policies and complying with the Act.

LAWYER CONTACTS

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com.

Fernando de Ovando
Mexico City
+52.55.3000.4010
fdeovando@jonesday.com

Mauricio F. Paez
New York
+1.212.326.7889
mfpaez@jonesday.com

ENDNOTES

1 No official English translation of the Act was available during the writing of this *Commentary*.

2 *Ley Federal de Protección de Datos Personales en Posesión de los Particulares* [L.F.P.D.P.] [Federal Law for Protection of Personal Data held by Private Persons], *Diario Oficial de la Federación* [D.O.F.], 5 de Julio de 2010 (Mex.).

3 The word "legitimate" is not defined in the Act.

4 LFPDP art. 22.

5 LFPDP art. 20.

6 Currently known as the Federal Institute of Access to Public Information.

7 LFPDP art. 38.

8 LFPDP art. 45.

9 LFPDP art. 51.

10 LFPDP art. 56.

11 LFPDP art. 64, 67-69.

12 LFPDP art. 2.

13 *Id.*

14 The Act uses the word "tratamiento," which literally translates to "treatment" in English. However, purposes of this *Commentary*, we use the word "processing" as it most accurately encompasses the definition provided in the Act. LFPDP art. 3, subsection XVIII.

15 LFPDP art. 3, subsection XVIII.

16 *Id.*, subsection V.

17 *Id.,* subsection VI.

18 *Id.*

19 LFPDP art. 7.

20 LFPDP art. 16 IV, 28, 29, 32.

21 LFPDP art. 8.

22 LFPDP art. 9. Also, the implementing of any electronic signature and authentication method must comply with the relevant provisions of the Civil Code, the Civil Procedures Code, the Commerce Code, and the Consumer Protection Law (modified as part of Mexico's e-commerce amendments in 2000).

23 *Id*.

24 *Id*.

25 LFPDP art. 18.

26 LFPDP art. 16.

27 *Id*.

28 LFPDP art. 11.

29 *Id*.

30 LFPDP art. 13.

31 LFPDP art. 12.

32 LFPDP art. 11.

33 LFPDP art. 14.

34 *Id.*

35 *Id*.

36 LFPDP art. 19.

37 *Id*.

38 LFPDP art. 20.

39 LFPDP art. 21.

40 *Id*.

41 LFPDP art. 27 and 29.

42 LFPDP art. 25.

43 *Id.*

44 *Id*.

45 LFPDP art. 30

46 LFPDP art. 32

47 *Id*.

48 *Id*.

49 LFPDP art. 33.

50 LFPDP art. 35.

51 Under the Act, all cost and fine calculations rely on the Federal Daily Minimum Wage scheme. Mexico applies three different federal daily minimum wage amounts to each of three geographical regions, labeled A, B, and C. For the purpose of this *Commentary*, we calculate the USD amount based on Geographical Area "A," which applies the current highest federal daily minimum wage ($57.46 MXN). Mexico Facts and Figures, http://www.mexperience.com/discover/discov__ff.htm (last visited May 20, 2010).

52 LFPDP art. 35.

53 LFPDP art. 25.

54 *Id.*

55 LFPDP art. 36.

56 *Id.*

57 LFPDP art. 37.

58 LFPDP art. 14, 38, 39, 45, 59.

59 LFPDP art. 45.

60 *Id.*

61 LFPDP art. 48.

62 LFPDP art. 56.

63 LFPDP art. 59.

64 *Id.*

65 LFPDP art. 60.

66 LFPDP art. 65.

67 LFPDP art. 64.

68 *Id.*

69 *Id.*

70 *Id.*

71 *Id.*

72 LFPDP art. 67.

73 LFPDP art. 68.

74 LFPDP art. 69.