MORRISON | FOERSTER

Morrison & Foerster Client Alert.

November 15, 2010

International Data Protection Laws

By Cynthia Rich, Naghmeh Ordikhani and Miriam Wugmeister

INTERNATIONAL DATA PROTECTION LAWS

In the past year, three more countries — Mexico, Malaysia, and Taiwan — have adopted comprehensive national privacy laws that regulate the collection, use, and disclosure of personal information. These new privacy laws differ considerably from those in the United States. U.S. laws typically focus on addressing misuse of information and seek to protect individuals from particular harms. These three laws instead are omnibus laws that extend protections to all personal information and focus not only on the use of information but also on the collection and disclosure of personal information. With the addition of these three new international laws, there are now almost eighty countries with comprehensive privacy laws in effect, many of which have their own unique regulatory requirements. The addition of each new foreign law poses greater compliance challenges for global organizations. This article provides an overview of the requirements contained in the data privacy laws recently adopted in Mexico, Malaysia, and Taiwan.

MEXICO

Overview

In July 2010, Mexico approved the Federal Law on Protection of Personal Data Held by Private Parties (the "Mexican Law"). The Mexican Law contains many of the basic obligations that are found in data protection laws around the world.

The law applies only to private parties but does not apply to duly licensed credit reporting companies or to persons who collect and store personal data exclusively for personal use.

Both the regulatory body charged with regulating the law, the Federal Public Information and Data Protection Institute (IFAIPD), and the requisite implementing regulations are expected to be in place by January 2012.

Definition of Personal Information

The Mexican Law applies to all personal information that concerns an identified or identifiable individual. The Mexican Law also classifies certain information as sensitive personal information, which is subject to additional (*i.e.,* notice and

Beijing

Paul D. McKenzie	86 10 5909 3366
Jingxiao Fang	86 10 5909 3382

Brussels

Karin Retzer	32 2 340 7364
Joanne Lopatowska	32 2 340 7365
Antonio Seabra Ferreira	32 2 340 7367

Hong Kong

Gordon A. Milner	852 2585 0808
Nigel C.H. Stamp	852 2585 0888

Los Angeles

Mark T. Gillett	(213) 892-5289
Michael C. Cohen	(213) 892-5404
David F. McDowell	(213) 892-5383
Russell G. Weiss	(213) 892-5640

London

Ann Bevitt	44 20 7920 4041
Anthony Nagle	44 20 7920 4029
Chris Coulter	44 20 7920 4012
Suzanne Horne	44 20 7920 4014

New York

Gabriel E. Meister	(212) 468-8181
Joan P. Warrington	(212) 506-7307
John F. Delaney	(212) 468-8040
Madhavi T. Batliboi	(212) 336-5181
Suhna Pierce	(212) 336-4150
Marian A. Waldmann	(212) 336-4230
Miriam Wugmeister	(212) 506-7213
Sherman W. Kahn	(212) 468-8023

Northern Virginia

Daniel P. Westman	(703) 760-7795
Timothy G. Verrall	(703) 760-7306

Palo Alto

Bryan Wilson	(650) 813-5603
Christine E. Lyon	(650) 813-5770

San Francisco

Roland E. Brandel	(415) 268-7093
James McGuire	(415) 268-7013
William L. Stern	(415) 268-7637
Jim McCabe	(415) 268-7011

Tokyo

Daniel P. Levison	81 3 3214 6717
Jay Ponazecki	81 3 3214 6562
Toshihiro So	81 3 3214 6568
Yukihiro Terazawa	81 3 3214 6585

Washington, D.C.

Andrew M. Smith	(202) 887-1558
Cynthia J. Rich	(202) 778-1652
Julie O'Neill	(202) 887-8764
Nathan David Taylor	(202) 778-1644
Obrea O. Poindexter	(202) 887-8741
Reed Freeman	(202) 887-6948
Richard Fischer	(202) 887-1566
Kimberly Strawbridge Robinson	(202) 887 1508

consent) requirements. Sensitive personal information is information relating to the most "private areas of the data owner's life" or "whose misuse might lead to discrimination or involve a serious risk" to the individual. Specific examples of sensitive personal data include the following information: (1) racial or ethnic origin; (2) existing and future health status; (3) genetic information; (4) religious, philosophical, and moral beliefs; (5) union membership; (6) political views; and (7) sexual orientation.

Appointment of a Data Protection Officer or Office

The Mexican Law requires any entity that collects personal information (the "data controller") 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.

Privacy Notice

At the time personal information is collected from individuals, the data controller 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 data controller 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.

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 or electronic signature or any other authorization mechanism established for the purpose. In general, the form of the consent can be verbal, written, electronic, or optical. If the data controller intends to process personal information for another purpose which is not compatible with or analogous to the purposes set out in the privacy notice, a new consent from the individual must be obtained.

Data Security

The Mexican Law also requires that the data controller establish and maintain physical, technical, and administrative security measures to protect personal data from damage, loss, alteration, destruction, or unauthorized use, access, or processing. Data controllers 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.

Data Integrity

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

Data Retention

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

As of January 6, 2012, 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 data controller must notify the individual within twenty days from receipt of a request what actions the data controller will take with respect to the personal information and then must implement the request to correct or delete or update data within 15 additional days.

Data Transfer to Third Parties

If personal information will be transferred to domestic or foreign third parties, the data controller 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 data controller.

In certain cases, domestic or international transfers of data may be carried out without the consent of the individual. For example, data may be transferred without consent to affiliated entities that operate under the same internal processes and policies as the data controller or under common control of the data controller. Consent is also not required where the transfer is necessary to complete a contract between the data controller 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 Requirements

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 data controller 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 $1.4 million). Up to 5 years imprisonment is also possible for crimes relating to the unlawful processing of personal data.

MALAYSIA

Overview

The Personal Data Protection Act 2010 was given Royal Assent and published in the *Gazette* in June 2010; however, the Act will only come into operation on a date determined by the Minister of Information, Communication, and Culture. No date has been set but the Personal Data Protection Commission is expected to be set up by the end of 2010 or beginning of 2011. Implementing regulations will then need to be issued. Once the Act enters into force, private sector organizations will have three months to comply.

This Act establishes comprehensive rules for the processing of any personal data "by private sector entities in respect of *commercial transactions*." Commercial transactions are defined as "any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance, but does not include a credit reporting business carried out by a credit reporting agency under the Credit Reporting Agencies Act 2009." One key question for organizations is whether this Act will apply to the processing of employee data. Until the Malaysian Act enters into force and guidance is issued by the regulatory authority, this question will remain unanswered.

The Malaysian Act will apply to all other data processing by private sector entities that are established in Malaysia or, if not established in Malaysia, use equipment in Malaysia for processing personal information. The Malaysian Act does not apply to Malaysia's federal and state governments.

Definition of Personal Information

Personal information includes any information with respect to commercial transactions that relates "directly or indirectly" to a data subject, who is "identified or identifiable from that information or from that and other information in the possession of" the data user (data controller). This includes sensitive personal information, which is defined as personal information relating to the physical or mental health or condition of a data subject or his or her "political opinions, religious beliefs, or other beliefs of a similar nature."

Notice

A data controller must provide data subjects with a written notice that advises them that their personal information is being processed and provides them with a description of that information, the purposes for which it is being processed, the class of third parties to whom their personal information may be disclosed, and the source of the personal information. In addition, the notice must explain the data subject's access and correction rights, the way to contact the data controller with any inquiries or complaints, the choices and means the data controller offers for limiting the processing of the data subject's personal information, whether it is obligatory or voluntary for the data subject to provide the information, and the consequences if the data subject refuses to provide the personal information.

Notice should be given as soon as "practicable" by the data controller, which could mean when the data subject is first asked to provide the information or when the data controller first collects the personal information. The notice must be given, however, before the data collector uses the personal information for a purpose other than the purpose for which the personal information was collected, or before the data collector discloses the personal information to a third party.

Consent

Subject to limited exceptions, explicit consent is required to process sensitive information; consent (undefined) is required for non-sensitive information. A data subject may withdraw consent by providing the data controller with a written notice stating the objection to the processing of personal information. In addition, a data subject may, at any time by written notice, require data controllers to cease or to not begin processing personal information for direct marketing purposes.

The exceptions for the processing of sensitive data contained in the Malaysian Act are similar to those found in many European laws. For example, consent is not required where processing is necessary to protect vital interests, obtain legal advice, administer justice, or provide medical care. In addition, consent to process sensitive data is not required in order "to exercise or perform any right or obligation permitted or required by law in connection with employment." This latter exception suggests, despite the previously discussed ambiguity about whether the processing of employee data falls within the scope of the Malaysia Act, that employee data may in fact be covered; however, until the authorities issue guidance, the full scope of the law remains unclear.

Finally consent to process non-sensitive personal information is not required if the information has been made public as a result of steps deliberately taken by the data subject.

Data Security

The data controller must take "practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction." A variety of factors such as the nature of the personal information and the harm that could result from such a misuse of the personal information should be taken into account when adopting security measures. Where personal information is to be processed by a data processor, the data controller must ensure that the data processor provides sufficient guarantees regarding the security measures it will take, and must supervise compliance with those security measures.

Data Integrity

The data controller must take reasonable steps to ensure that the personal information is accurate, complete, not misleading, and up-to-date for the purposes (including any directly related purpose) for which the data was collected and further processed.

Data Retention

In addition, the data controller must ensure that all personal information is destroyed or permanently deleted if it is no longer required for the purpose in which it was collected.

Access and Correction Rights

Subject to certain exceptions, data subjects must be given access to their personal information held by a data controller and be able to correct that personal information where inaccurate, incomplete, misleading, or not up-to-date. Access requests are to be made in writing and a fee may be charged for such requests. The data controller must keep and maintain a record of such requests; the Personal Data Protection Commissioner may determine the manner and form in which the record is to be maintained.

Data Transfers Outside of Malaysia

A data controller may not transfer any personal information to a place outside Malaysia unless the jurisdiction is listed in a notification issued by the Minister of Information and published in the *Gazette* or an exception applies. The approved jurisdictions must have in place laws that are substantially similar to the Malaysian Act or must ensure an adequate level of protection that is at least equivalent to the level of protection afforded by the Malaysian Act.

Alternatively, transfers to places outside Malaysia may occur if one of the listed exceptions applies. Some of these exceptions are similar to those found in European laws such as: the data subject has consented to the transfer; the transfer is necessary to carry out a contract between the data controller and the data subject; the transfer is necessary to conclude or carry out a contract between the data controller and a third party at the request of the data subject; or the transfer is in the interests of the data subject.

Lastly, there is another exception listed which may be useful for organizations that develop APEC cross-border privacy rules ("CBPRs").[1] Transfers outside of Malaysia will be permitted in cases where the data controller "has taken all reasonable precautions and exercised all due diligence to ensure the data will not in that place be processed in any manner which, if that place is Malaysia, would be a contravention of this Act." Further guidance from the regulatory authority is needed, however, to clarify what measures will satisfy the conditions set forth in this exception.

Database Registration Requirements

While the Malaysian Act establishes detailed registration requirements, it does not specify to whom such obligations would apply; rather, it gives the relevant Minister the authority to designate a class of data controllers that will be required to register under this Malaysian Act. Consequently, until the regulatory authority is established, it remains unclear which types of organizations, if any, will be subject to registration obligations.

Penalties

Violations of the Malaysian Act, such as unlawful processing of sensitive personal information, transfers to jurisdictions not approved by the Minister, or failure to honor a request to cease processing, can result in up to 2 years of imprisonment, a fine up to 200,000 ringgit, or both. Unlawful collection, disclosure or sale of data is punishable by imprisonment up to three years, a fine up to 500,000 ringgit, or both.

TAIWAN

Overview

In 1995 Taiwan adopted a Computer Processed Personal Data Protection Act (the "CPPDPA"). That law covered data in specific sectors such as financial, telecommunication, and insurance and only covered computerized data. In April 2010,

[1] Asia-Pacific Economic Cooperation ("APEC") is an inter-governmental forum consisting of 21 Member Economies. It was established in 1989 to further enhance economic growth and prosperity for the region and to strengthen the Asia-Pacific community. One of its goals is to facilitate a favorable and sustainable business environment. The APEC Electronic Commerce Steering Group is developing a system for cross-border data flows among APEC members to implement its 2005 Privacy Framework. See APEC, Data Privacy Pathfinder Projects Implementation Work Plan, http://www.apec.org/apec/apec_groups/committee_on_trade/electronic_commerce.html.

Taiwan amended that law with the Personal Data Protection Act (the "PDPA"). The PDPA now provides protection to personal data across all public and private entities and across all sectors.

The PDPA will only become effective when the Executive Yuan, the central government administrative authority, issues an official order that specifies its effective date. According to government authorities, the PDPA should become effective by November 2011.

Definition of Personal Information

The PDPA has expanded the CPPDPA definition of personal information to include not only computer-processed personal information but also personal information in any data format. Personal information now includes any information that refers to a "natural person's name, date of birth, national unified ID card number, passport number, characteristics, fingerprint, marital status, family, education, occupation, medical history, medical treatment, genetic information, sex life, health examination, prior criminal records, contact information, financial status, and social activities as well as other data which can be used directly or indirectly to identify" this natural person.

Collection Limitations

Unlike the CPPDPA which does not forbid the collection or use of any specific kind of personal information, the PDPA prohibits anyone from collecting, processing, or using sensitive personal information except in very narrow circumstances. Sensitive personal information is defined as medical treatment, genetic information, sex life, health examination, and prior criminal records. In particular, sensitive personal information may only be processed when: 1) explicitly required by law; 2) necessary to carry out a statutory obligation (and only provided appropriate security measures are in place); 3) made public by the data subject or through other legal methods; or 4) carried out by a government agency or academic research institute for medical purposes, crime prevention, research, or statistical purposes. The PDPA authorizes the central competent authorities and the Ministry of Justice to develop regulations regarding the processing of sensitive information.

The collection limitations on non-sensitive information remain largely the same as under the existing law. In particular, non-sensitive personal information may be collected and processed only for a specific purpose, when, for example: 1) the information is explicitly required by law; 2) the private sector organization is engaged in a contractual or quasi-contractual relationship with the data subject; 3) the written consent of the data subject has been obtained; or 4) the personal information has been made public by the data subject or through other legal methods. In addition, personal information may be used for a different purpose but only when, for example: 1) the information is expressly required by law; 2) necessary to avoid danger to the life, body, freedom, or property of the data subject or to prevent serious damage to the rights and interests of others; or 3) the written consent of the data subject has been obtained.

Notice

Subject to certain exceptions, notice must be provided to data subjects when personal information is collected from them and must include information such as the name of the entity that is collecting the information, the purposes of collection and use, the type of information to be collected, and the duration of use of the information. Data subjects must also be informed of their access and correction rights. If personal information is not collected directly from the data subject, notice must be provided to the data subject prior to processing or using and the data subject must be advised about the source of the personal information being collected.

Consent

Where consent is to be obtained, it must be in writing and only after the requisite notice has been provided. If personal information is to be used for a different purpose than described in the notice, and consent will be used as the legal basis for this new use, then a separate written consent must be obtained from the data subjects after they have been expressly informed about the different purpose and the effect their consent or refusal will have on their rights and interests.

Data Security

Private sector organizations that hold personal information are required to adopt appropriate security measures to prevent information from being stolen, altered without authorization, destroyed, eliminated, or divulged. The competent authority responsible for regulating a specific industry may require organizations subject to its oversight to develop data security maintenance plans or data disposal procedures.

Data Integrity

Private sector organizations must maintain the accuracy of the personal information, supplementing or correcting the information on their own initiative or upon request from the data subject.

Data Retention

When the purpose of collection has been fulfilled or the period in which the personal information may be used has expired, the private sector organization must delete or discontinue processing the information or it must delete the information when requested to do so by the data subject, unless the processing or use is necessary to perform a business operation or a written consent of the data subject has been obtained.

Access and Correction Rights

Subject to a number of exceptions, a data owner whose personal information has been processed has the right to: (1) access; (2) review; (3) receive duplicates of; (4) cancel the collection, processing, or utilization of; and (5) delete the personal data. These rights cannot be waived in advance or limited by an agreement. The PDPA requires that access requests be acted on within 15-30 days. Correction requests must be acted upon within 30-60 days. Organizations may at their own discretion charge a fee to cover the costs associated with responding to such requests.

Data Transfers Outside Taiwan

There are no explicit cross-border restrictions contained in the amended law; however, the PDPA does give government agencies the authority to restrict international transfers in the industries they regulate, under certain conditions such as when: (1) the transfer involves a major national interest; (2) there are special provisions in a international treaty or agreement restricting the transfer; (3) the receiving country does not yet have proper laws and regulations to protect personal data so that the data owner's rights and interests may be damaged; and (4) personal data are indirectly transmitted to a third country to evade this Act.

Database Registration Requirements

Under the CPPDPA, organizations had the obligation to file a registration and obtain a license. The PDPA abolishes the CPPDPA's previous registration requirements and there are no obligations to file registration with any authority.

Breach Notification

In the event that the data controller has violated provisions of the PDPA, causing personal data to be stolen, divulged, or altered without authorization, or infringed upon in any way, the data controller must notify the data subject after an investigation has been completed.

Penalties

The PDPA significantly strengthens the penalties that can be imposed on organizations that violate the law. For example, organizations that profit from the collection, processing, or use of personal data can be fined up to NT$1 million (compared to NT $40,000 under the CPPDPA) or face a term of imprisonment of up to 5 years (versus 2 years under the CPPDPA). Depending on the gravity of the violation, damages of NT$ 500-2,000 may also be claimed per violation of the PDPA even if the actual damage cannot be proven. In addition, class action suits will be permitted.

IMPLICATIONS

The new laws in Mexico, Malaysia, and Taiwan significantly change the privacy landscape in these countries. Organizations should carefully examine their existing data privacy practices and procedures to ensure they comply with these new laws. Failure to comply with these laws can result in significant civil and criminal penalties.

For many organizations, it will mean that in these countries they will have to issue privacy notices, obtain consent to process, use, and transfer personal information, establish mechanisms for individuals to exercise their access and correction rights, and ensure that their data security and retention policies and practices conform to the laws' requirements. In addition, organizations in Mexico and Taiwan will now have an obligation to notify individuals in the event of a data security breach.

Moreover, in Malaysia and Taiwan, organizations may be subject to specific cross-border limitations which will further complicate their efforts to transfer and share data within their global organizations. Consequently, they may have to establish new legal mechanisms to enable such transfers to continue. Organizations also need to examine their data collection practices, particularly in Taiwan, to ensure that their practices comply with the collection limitations set forth in the law.

Organizations should assess their data privacy practices and procedures in these countries and begin to formulate compliance plans, bearing in mind, however, that it will be difficult to finalize compliance efforts until these laws become fully effective and implementing regulations and regulatory guidance are issued by the authorities.

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials in many areas. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer*'s A-List for seven straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations.