

Privacy Primer

An Overview of Global Data Protection Laws

© Copyright 2007. Hunton & Williams LLP All rights reserved.

The White Paper is provided for educational purposes only with the understanding that the publisher is not engaged in rendering legal, medical, insurance or other professional services through its distribution.

This Paper is not intended to substitute for professional advice. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

Privacy Primer

An Overview of Global Data Protection Laws

TABLE OF CONTENTS

INTRODUCTION	1
SCOPE.....	1
THE EUROPEAN UNION	1
A. Introductory Concepts	2
B. Legal Instruments and Basic Principles.....	2
1. General Directive	3
2. Directive on Privacy and Electronic Communications	3
3. Data Retention Directive.....	4
C. Practical Implications of Data Protection Law	4
1. Data Processing Registrations.....	4
2. International Data Transfers	5
3. Direct Marketing.....	6
D. Enforcement of the Law	6
E. Conclusion.....	7
ASIA PACIFIC.....	8
A. Australia	8
B. Hong Kong	10
C. India.....	11
D. Japan.....	11
E. People’s Republic of China	13
F. Singapore.....	14
G. South Korea.....	14
H. Thailand.....	15
CANADA	16
A. Applicability	16
B. PIPEDA’S Requirements	17
C. Investigation, Enforcement and Penalties.....	18
D. Ontario.....	18
LATIN AMERICA	19
A. Argentina	19
B. Chile	20
C. Mexico.....	20
AFRICA.....	22
SOUTH AFRICA	22
A. Common Law/Constitutional Right to Privacy	22
B. Contractual Right to Privacy	22
C. The Promotion of Access to Information Act, 2000 (“PAIA”)	22
D. The Electronic Communications and Transactions Act, 2002 (“ECTA”)	23
E. The National Credit Act	23
CONCLUSION.....	23

INTRODUCTION

Privacy and data protection laws exist in many countries overseas. In numerous other countries, privacy laws are under consideration. Where privacy laws are in place, some are relatively new while others are more mature. Few are more than 10 years old. As these laws have matured, government enforcement has increased. Public interest also has grown; surveys show that consumers consider corporate information practices when choosing service or product providers. Consequently, as U.S. companies expand overseas, privacy and data protection considerations must form a key component of global compliance programs and worldwide business strategies.

International privacy laws often differ considerably from their U.S. counterparts in their scope and application. In particular, while U.S. privacy laws tend to be sectoral in nature, impacting only certain industries, laws overseas often are comprehensive in scope. Outside the EU, where all member countries have similar data protection laws, there is little uniformity when comparing the data protection regimes of various jurisdictions.

Data protection laws typically apply to both customer personal information and employee data. The laws sometimes require conduct that is both burdensome and unusual in the U.S. (for example, in the EU, companies generally must register their databases with the government. It is important to consult with a data protection expert before attempting to collect, process or disclose employee or consume personal information overseas, and before granting access to those data to individuals located outside the jurisdiction.

Enforcement of foreign data protection laws often is less visible and more sporadic than enforcement in the U.S. In the U.S., violations of privacy and data security requirements can result in fines or penalties, and such events tend to be highly publicized. In other countries, local authorities may quietly manage privacy violations but, instead of imposing penalties, these authorities may impose equitable remedies, such as enjoining any further use or collection of individuals' data. This result can cause significant hardship to the business whose data processing has been enjoined. In addition, in certain countries, criminal penalties (including imprisonment) could result from violations of data protection laws.

In light of the global nature of information, and the ease and speed with which personal data travels around the world, a trend toward global harmonization of data protection principles is inevitable. Such harmonization is not imminent, however. With many countries just beginning to enact and enforce their own privacy laws, it is clear that this nascent area of the law has not yet matured sufficiently to expect global uniformity. Until basic data protection principles are universally embraced, businesses will need to contend with widely varied regulatory schemes worldwide.

SCOPE

This primer was prepared by members of the Privacy and Information Management Team of Hunton & Williams LLP to assist the members of the Mortgage Bankers Association in increasing awareness of global data protection laws. This primer does not address U.S. law. Rather, it describes the data protection laws that are most relevant to businesses that are expanding beyond the U.S. This guide addresses the principal data protection laws in countries that are most frequently encountered by international businesses.

THE EUROPEAN UNION

European data protection law has its origins in human rights treaties and various national constitutions. Data protection is regarded in Europe as a fundamental human right. In a groundbreaking judgment rendered in 1983, the German Federal Constitutional Court recognized a "right to informational

self-determination,” which is also recognized in various human rights treaties concluded by the European nations.

The European Union (“EU”) was the first legal system in the world to produce a comprehensive, omnibus approach to privacy and data protection that covers all industry sectors and all types of data processing. The EU currently is comprised of 25 European countries, or “Member States,” though the number is expected to increase. The EU provides the legal framework for data protection in Member States by the passage of so-called “directives,” which Member States are then required to implement by enacting and enforcing national laws that embody the directives. Private entities and other parties are required to comply with the national laws, which may vary in their implementation of the EU directives. National regulatory bodies commonly referred to as data protection authorities, or “DPAs,” enforce the national laws.

EU data protection law has several key features, such as the creation of a minimum level of data protection for individuals and the elimination of restrictions on data transfers among EU Member States based on the level of data protection provided in national law. Businesses often find the rules of EU data protection law overly bureaucratic (e.g., rules on registering databases with DPAs), inflexible and burdensome (e.g., rules on international data transfers). There is also insufficient harmonization among Member State data protection laws.

A. Introductory Concepts

European data protection law is replete with complex legal terminology, which can often make it difficult to understand. Among the most important terms are “personal data,” which is the information protected by EU data protection law. “Personal data” is defined as “any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.” The concept of personal data is quite broad and includes almost any type of data that could ever be tied to an identified or identifiable individual. Also of importance is the term “data processing,” which is “any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.” Related concepts include “data controllers,” the entities with the authority to direct how the data are processed (usually the business that “owns” the data), and “data processors,” the third parties that process personal data under the direction of data controllers. The individuals whose personal data are processed and, as such, receive the legal protections described in this guide are referred to as “data subjects.” Any individual residing in Europe is potentially a data subject, including a company’s employees, customers, or other individual business contacts.

B. Legal Instruments and Basic Principles

EU data protection law is governed primarily by three directives: (1) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the “General Directive”); (2) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning processing of personal data and the protection of privacy in the electronic communications sector (the “Directive on Privacy and Electronic Communications”); and (3) Directive 2006/24/EC of the European Parliament and the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 92006) OJ L105/54 (the “Directive on Data Retention”). As discussed above, each EU Member State is required to enact national laws giving force and effect to these directives.

1. General Directive

The major instrument of EU data protection law is the Data Protection Directive, or “General Directive,” adopted on October 24, 1995. The General Directive is founded on six primary principles:

- *Legitimacy:* Personal data may only be processed for limited, legitimate purposes.
- *Finality:* Personal data may only be collected for specified, legitimate purposes and may not be further processed for any incompatible purpose.
- *Transparency:* Data subjects must receive information about the processing of their personal data.
- *Proportionality:* Personal data must be relevant and not excessive in relation to the purpose for which they are collected and processed.
- *Confidentiality and security:* Technical and organizational measures appropriate to the risks presented by the data processing must be in place to ensure the confidentiality and security of personal data; and
- *Control:* Data protection authorities must enforce data protection law.

Under the General Directive, personal data should be used only for purposes to which the individual has consented or for purposes that would be reasonably obvious to the individual on the basis of the information provided at the time the data was initially collected. Explicit consent is virtually always required when the personal data are deemed “sensitive.” Sensitive personal data are defined as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. Some Member States also view criminal histories or drivers’ records as sensitive personal data.

Data subjects must be provided with certain information when their data are collected for processing, including: (1) the identity of the entity processing the data; (2) confirmation that their data will be processed and information regarding the purposes of the processing; (3) the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed; (4) the logic involved in any automatic data processing; and (5) their right to request rectification of inaccurate data, erasure or blocking of data processing that does not comply with the Directive, and notification of the identity of any third parties to whom the data have been disclosed.

2. Directive on Privacy and Electronic Communications

The Directive on Privacy and Electronic Communications addresses data protection in the electronic communications sector, which includes telecommunications, faxes, e-mail, the Internet, and similar services. Specifically, this Directive applies to personal data processed in “publicly-available electronic communications services in public telecommunications networks in the Community.” Providers of such services must take appropriate technical and organizational measures to safeguard their systems and services. Member States are to ensure the confidentiality of communications by national legislation, though limited exceptions are provided where government wiretapping activities and national security interests necessitate disclosure. Among other provisions, the processing of traffic and billing data are subject to further restrictions. In particular, data subjects are given specific rights with regard to itemized billing, calling line identification, call forwarding, directories, and unsolicited calls.

3. *Data Retention Directive*

In the EU, Member States often obligate providers of publicly available electronic communications services to retain certain data, primarily communications traffic data, to ensure that such data are available for purposes such as law enforcement and national security. The Data Retention Directive, recently passed, attempts to harmonize the various retention requirements imposed by Member States. The Directive requires telecommunications companies to retain a wide range of data, including incoming and outgoing phone numbers (fixed and mobile), the duration of phone calls, IP addresses (dynamic and static), login and logoff times, and e-mail activity. The legislation allows Member States to decide how long data should be retained within a minimum of six and a maximum of 24 months from the date of communication. The data must be erased thereafter. Processing of the data during the period of retention must be carried out in accordance with the requirements of the General Data Protection Directive. Member States must implement the Data Retention Directive by September 15, 2007.

C. *Practical Implications of Data Protection Law*

EU data protection law has important practical implications for companies conducting business in the region. For instance, the transparency principle mandates that companies must notify both their customers and their employees of the types of personal data collected, the purposes for which they are processed, and the categories of recipients to whom the data may be disclosed. As a further example, the proportionality principle requires companies to consider carefully the types of personal data necessary to the companies' purposes and must limit their collection to only those data. The most significant and burdensome of the requirements are discussed below.

1. *Data Processing Registrations*

Companies doing business in the EU are often required to notify DPAs of their data processing activities, whether they conduct these activities or contract with a service provider to conduct them. Most Member States prescribe a registration procedure by virtue of which each DPA must be notified of any database containing personal data. Specific application forms may be employed by the DPA, the form and scope of which vary widely among Member States. For example, while registrations in the UK are often only a page or two in length, the application form used in Italy is 86 pages long. The process is further complicated by the usual requirement that these forms be submitted in the local language. Despite wide variation between Member States, the registration usually entail providing a contact person to communicate with the DPA and describing the type of personal data processed, data subjects affected, purposes of the processing, security applied to the data and any transfers or disclosures of the data.

Article 18(2) of the General Directive allows Member States to create exceptions to the registration requirement when implementing the Directive. Some national data protection legislation does provide exceptions, but the availability of these exceptions varies widely among Member States. One of the more common exceptions is provided when a company has appointed a data protection officer to safeguard personal data processed by or on behalf of the company. The laws of France, Germany, Luxembourg, Sweden and The Netherlands provide for such an exception. Usually, the company must notify the DPA of the data protection officer's appointment, and that officer is required to keep inventories of the data processing activities that would otherwise have been registered with the DPA. These inventories could, in principle, be reviewed by the DPA in the event of an inspection. The company must ensure that, if the data protection officer is to have other job responsibilities, these may not be inconsistent or create conflicts of interest with the responsibility to uphold EU data protection principles.

2. *International Data Transfers*

Among the restrictions of greatest importance to companies are those pertaining to the international transfer of personal data. Personal data may not be transferred to countries outside the EU unless there is a “legal basis” for the transfer. There are several possible grounds that may provide a legal basis for a transfer of personal data to a non-EU country. First, the European Commission may issue an official “adequacy finding,” determining that the country in question offers an adequate level of data protection on the basis of its national laws. Since the enactment of the General Directive, only a very small number of such adequacy determinations have been issued, covering Argentina, Canada, Guernsey, the Isle of Man, and Switzerland.

There are several other potential legal bases for international data transfers in cases where the country to which personal data will be sent has not received an adequacy finding. The most important such legal bases are the following:

- The consent of the individual whose data are being transferred. However, consent can be difficult to manage in practice (e.g., since consent may be revoked), and may not be considered legally valid, particularly in the employment context, in which consent is sometimes considered coerced.
- Execution of the EU-approved “standard contractual clauses.” These standardized data transfer agreements are concluded between the “data exporter” (the entity in the EU) and the “data importer” (the entity outside the EU), which agree to grant certain protections to the data. The clauses have been given an adequacy finding by the EU, and so may not be modified by the signing parties; rather, the parties are required to describe the nature of their data transfer in an annex to the clauses. Some countries require the executed clauses to be filed with the DPA, and several require affirmative approval from the DPA prior to the transfer. As such, the clauses are difficult to use in practice, particularly when a company seeks to transfer personal data to hundreds of its subsidiaries worldwide, which would require each entity to execute the clauses.
- The fact that the transfer may be necessary for the performance of a contract between the entity transferring the personal data outside the EU and the individual whose data are being processed. This legal ground is construed narrowly and is useful only in certain narrowly defined situations (e.g., when a person in Europe has made a hotel booking for a foreign vacation and data about his stay needs to be transferred to the hotel outside the EU where he will be staying).
- The U.S. safe harbor program, which is a voluntary, self-regulatory scheme that has received an adequacy finding from the EU. Companies choosing to join the program must certify their compliance on an annual basis. The program is available only to entities that are subject to Federal Trade Commission jurisdiction, and so only provides a legal basis for transfers of personal data from the EU to safe harbor-certified entities in the U.S.
- Implementation of “binding corporate rules,” or BCRs. BCRs are a set of data processing rules and principles adopted by a company or group of companies that bind all of the company’s entities worldwide to abide by certain protections. BCRs must be approved by DPAs but, once approved, allow the legal international transfer of personal data among the entities bound to comply with the BCRs. Through the use of BCRs, the entire corporate group essentially becomes a “safe haven” in which personal data can be freely transferred

from one corporate member to another, receiving the same protection wherever it goes and shifting the burden of ensuring compliance to companies themselves.

The EU restrictions on international data transfers have significant economic implications. Many companies in Europe spend considerable time and money complying with these restrictions. They can have particularly serious consequences for outsourcing transactions, since a company in Europe may not transfer personal data to, for example, China or India for outsourcing purposes unless a valid legal basis for the transfer is present. This often adds considerable cost and complexity to outsourcing transactions.

3. Direct Marketing

The Directive on Privacy and Electronic Communications directs Member States to allow unsolicited commercial telephone calls, e-mails and faxes only with the prior consent of the recipient. Two types of consent are recognized in the EU. “Opt-in,” or explicit, consent is obtained when the data subject affirmatively indicates her preference to receive marketing communications. “Opt-out” consent is obtained when the data subject is presented with an opportunity to object to receiving marketing communications, but does not.

<p>Opt-in consent:</p> <p>By ticking the box below, you consent to allow COMPANY to send you e-mails to let you know about COMPANY’s products and services.</p> <p><input type="checkbox"/> I consent to allow COMPANY to send me e-mails about COMPANY’s products and services.</p> <p>Opt-out consent:</p> <p>Unless you tick the box below, COMPANY will send you e-mails to let you know about COMPANY’s products and services.</p> <p><input type="checkbox"/> I do not consent to allow COMPANY to send me e-mails about COMPANY’s products and services.</p>

The media in which marketing communications are sent will dictate the form of consent that must be obtained. Though the requirements vary by Member State (as with most areas of EU data protection law), opt-in consent usually is required prior to sending faxes or placing telephone calls. Opt-in consent also typically is required prior to sending unsolicited e-mail communications. An exception is made for marketing e-mails sent to data subjects with whom a company already has an “existing business relationship.” In that circumstance, the company is considered to have obtained “soft opt-in” consent from the data subject if the contact information was obtained in the course of a sale, contracting, or negotiations and the proposed communication pertains to products and services similar to those that were the subject of the existing business relationship. Regardless of the type of consent obtained at the outset, every direct marketing message sent subsequently must contain a mechanism to enable the data subject to opt out of receiving further messages, at little or no cost to the data subject.

D. Enforcement of the Law

Data protection enforcement in the EU is often less visible than enforcement actions in the U.S. Decisions of the DPAs are often not published and case decisions in European legal systems are usually

anonymized. Moreover, there is no doubt that the broad scope of EU data protection law in conjunction with the general lack of resources available to many national DPAs causes many violations of the law to go unpunished.

Nevertheless, there is an increasing amount of data protection enforcement in Europe, which can include criminal penalties, fines, injunctions, and adverse publicity. For instance, one decision from a German DPA required a major company to remove all cookies from its website, which significantly affected its online presence. The action was never made public, but the effect was just as serious as if the company had been forced to pay a large fine. A few other prominent examples of enforcement actions include:

- The Italian DPA investigated and prosecuted a company that illegally processed data for commercial solicitation. After discovering the company's failure to register its processing activity, the DPA issued an order blocking further data processing and reported the case to criminal court.
- The Spanish DPA imposed a fine of several hundred thousand Euros against a television producer who failed to appropriately secure a database containing the personal data of television show participants, and transmitted that data to third party advertisers without consent.
- A Finnish court ordered the jailing of several top executives of a large telecommunications company for illegally monitoring their employees' business telephones. The executives later received suspended sentences.

Most enforcement actions are initiated by DPAs, either in response to a complaint from an individual or on their own initiative. Individuals may also bring lawsuits based on data protection violations, but such lawsuits have been rare. Implementation of the General Directive has, however, given individuals an increased opportunity to file lawsuits directly against companies for misuse of personal data, since the Directive obligates Member States to create a direct cause of action.

Enforcement actions can cover a wide variety of legal violations. Among the most popular grounds for enforcement actions are failure to register data processing with the data protection authorities, sending unsolicited marketing material (particularly spam), and the transfer of personal data outside the EU without a valid legal basis. Employees and employee representatives are also often the source of complaints against employers for violations of data protection law.

E. Conclusion

EU data protection law was finalized just before the Internet age began in the mid-1990s, and this timing is reflected in a number of provisions of the General Directive that are difficult to reconcile with the demands of the online age (for example, the provisions dealing with determining applicable law, which are very difficult to apply in an online context). There is a lack of harmonization of even some of the most basic concepts of the General Directive (such as the definition of "personal data"), with different Member States implementing them in widely different ways in their national law. There is also no doubt that EU data protection law has a substantial impact on the day-to-day business practices of companies. Legal obligations such as the need to provide detailed notices to employees and customers, the need to register databases with the national data protection authorities, and restrictions on international data transfers involve substantial compliance costs for companies doing business in the EU.

ASIA PACIFIC

As countries in the Asia-Pacific region continue to expand their presence in the world economy, so too have these countries been increasingly enacting, or considering enacting, comprehensive privacy legislation. China's recent and ongoing efforts to identify a workable privacy framework have, in particular, captured the attention of both public and private entities worldwide. The following overview summarizes both significant and emerging privacy laws in the region.

A. Australia

Privacy law in Australia comprises several federal statutes covering particular sectors and activities, some State or Territory laws with limited effect, and residual common law protections. The principal federal statute is the Privacy Act of 1988, which gives partial effect to Australia's commitment to the Organization for Economic Cooperation and Development ("OECD") Guidelines. The Privacy Act sets forth eleven Information Privacy Principles, based on the principles articulated by the OECD Guidelines, that are applicable to most federal government agencies. A separate set of rules pertaining to consumer credit information was added to the law in 1989 and applies to all private and public sector organizations. In addition, the Privacy Act also regulates the use of government-issued Tax File Numbers by private and public entities. Finally, the National Privacy Principles ("NPPs") were commenced in December 2001, and have widespread application to private sector organizations.

The Privacy Act applies to the private sector by regulating the handling of personal information by "organizations." "Organizations" are defined to include individuals, corporate bodies, partnerships, any other unincorporated associations, or trusts. Acts and practices of individuals are exempt, however, if the act or practice is engaged in outside the course of the individual's business operations. Most small businesses are exempt with the exception of health care service providers, organizations that buy or sell information without individuals' consent, and contractors to federal government agencies to the extent of their contractual activities.

Most of the privacy protections available to Australians are provided by the NPPs. NPP 2 provides that personal information may only be disclosed for the primary purpose of collection. There are several exceptions. Among the most notable is the exception that disclosure for a secondary purpose is permitted if the secondary purpose is related to the primary purpose of collection and the individual would reasonably expect the organization to use or disclose the information for the secondary purpose. Disclosure for a secondary purpose is also permissible if the individual has consented to the use or disclosure. For example, if a company collects information about its employees for the primary purpose of compensating them and providing job-related benefits, it must seek their consent before using those contact details for the unrelated secondary purpose of sending marketing materials.

NPP 9 provides restrictions on the international transfer of personal information. These restrictions do not apply to an international transfer within an organization, nor do they apply to a transfer to the individual about whom the information relates. Under NPP 9, international transfers are only permitted if at least one of the following applies:

- the organization reasonably believes that the recipient of the information is subject to a law, binding scheme, or contract, which effectively upholds rules that are substantially similar to those imposed by the NPPs;
- the individual consents to the transfer;

- the transfer is necessary for the performance of a contract between the individual and the organization, or for the implementation of pre-contractual measures taken in response to the individual's request;
- the transfer is necessary for the conclusion or performance of a contract between the organization and a third party which is concluded in the interests of the individual;
- the transfer is for the benefit of the individual, it is impracticable to obtain the consent of the individual to that transfer and, if it were practicable to obtain such consent, the individual likely would give their consent; or
- the organization has taken reasonable steps to ensure that the transferred information will be held, used, or disclosed by the recipient in a manner consistent with the NPPs.

NPP 4 requires organizations to take reasonable steps to protect personal information from misuse, loss, and unauthorized access, modification or disclosure. NPP 4 does not require organizations to ensure that data processors acting on their behalf will handle personal information in accordance with the Privacy Act. Rather, if the data processor is subject to the Privacy Act (e.g., it is not exempt as a small business) then the processor has an independent obligation to comply with the Privacy Act. If an organization outsources data processing outside Australia, then the Privacy Act's restrictions on international data transfer will apply.

Australia's Privacy Act covers customer data processing but, with respect to processing of employee data, generally applies only to federal, public sector agencies. (Local laws, including local labor and privacy laws, may apply to processing employee data in the private sector.) The Privacy Act's exception with respect to private sector processing of employee data is relevant when the processing relates to the acts and practices of private entities that employ (or have employed) individuals and handle personal data pertaining directly to that employment relationship. The exemption expressly requires a direct relationship between the act or a practice and "a current or former employment relationship." The exemption, therefore, is not applicable with respect to unsuccessful applicants for employment or with respect to individuals not classified as employees.

The Privacy Act establishes the Office of the Privacy Commissioner, which is funded by the government but is otherwise rendered independent of the federal public service bureaucracy by statute. Under the Privacy Act, the Privacy Commissioner is appointed for a period not to exceed seven years. The Commissioner has a wide range of powers, including:

- investigating an organization's practices that may interfere with individual privacy and, if the Commissioner deems appropriate, reconciling the issues that gave rise to the investigation by settlement agreement;
- approving of an entity's privacy codes and amendments to approved privacy codes;
- acting as an independent adjudicator of complaints, which may be made under an approved privacy code;
- promoting greater understanding of and compliance with the NPPs;
- publishing guidelines to assist entities in complying with the NPPs, protecting the privacy of individuals, developing and applying privacy codes, and addressing complaints made under approved privacy codes; and

- developing a Credit Reporting Code of Conduct and investigating the practices of credit reporting agencies or credit providers that may constitute credit-reporting infringements.

The Privacy Act does not provide for substantive offenses or penalties in relation to the general rules applicable to organizations. Organizations may, however, be required to compensate individuals affected by any “interference with” their privacy. Procedural offenses provided under the Act may give rise to fines or imprisonment and include, for example, failure to attend a compulsory conference with the Privacy Commissioner, willful obstruction of an investigation by the Commissioner, knowing provision of false or misleading information to the Commissioner, and failure to provide any document or record to the Commissioner when such provision is required under the Privacy Act. These procedural offenses are intended to facilitate cooperation with investigations by the Privacy Commissioner, which are the primary method of enforcing the NPPs.

B. Hong Kong

Hong Kong enacted the Personal Data Privacy Ordinance (“PDPO”) in 1996. The PDPO applies to both public and private sector “data users.” The PDPO does not, however, apply to People’s Republic of China government agencies located in the Hong Kong Special Administrative Region under the Interpretation and General Clauses Ordinance. Following the standard set by the OECD 1980 Guidelines for Protection of Privacy and Transborder Flows of Personal Data, the PDPO adopted six “fair information principles” to regulate notice, collection, accuracy, use, security and access to “personal data,” broadly defined as “any representation of information (including an expression of opinion) in any document, that includes a personal identifier.” The PDPO requires that individuals be notified of the purposes of data collection, any prospective disclosures to third parties, and their right to access and correct their personal information. Data users are also required to make their data protection policies available to the public. Section 33 of the PDPO contains restrictions on the transfer of data to a location outside of Hong Kong, but the Ordinance was enacted without Section 33 going into effect.

The PDPO also imposes restrictions on certain processing, namely data matching (matching data to an individual) and direct marketing. The former requires prior approval from Hong Kong’s Privacy Commissioner for Personal Data, while the latter requires that a “data user” inform the individual of her opportunity to opt out from subsequent marketing messages. Hong Kong plans to enact an anti-spam law in 2006. The law, planned in consultation with industry groups, will make illegal unsolicited e-mails, junk faxes, and automated telemarketing calls. Fixed-line and mobile operators are actively involved in creating a code of practice for telemarketing.

The PDPO is supplemented by the Code of Practice on Human Resource Management (the “Code”), which provides a practical guide to the application of the PDPO to employment-related personal data protection. Non-compliance with the Code could give rise to a presumption against the employer, or any third party contracted in any proceedings involving an alleged breach of the PDPO. Also, non-compliance with the Code would weigh against the party concerned in any case under investigation by the Privacy Commissioner. In addition, the *Privacy Guidelines: Monitoring and Personal Data Privacy at Work* (the “Guidelines”) provide recommended standards of personal data management in the context of employee monitoring. The Guidelines are not definitive interpretations of the PDPO, but rather are standards recommended by the Privacy Commissioner, intended to offer practical solutions that balance legitimate business interests and employees’ personal data privacy rights.

Individuals may lodge complaints pertaining to alleged violations of the PDPO with Hong Kong’s Privacy Commissioner. The Commissioner may carry out enforcement activities, including issuing enforcement orders and monitoring compliance with the PDPO. Violations of the PDPO can result in either

criminal or civil penalties, with a maximum penalty of 1,000 Hong Kong dollars per day or two years imprisonment.

C. India

There is no comprehensive data protection law in India, though relevant provisions exist in sector-specific regulations. The Public Financial Institutions Act of 1993 codifies India's tradition of maintaining the confidentiality of bank transactions and prohibits unauthorized disclosures. Privacy in telecommunications is also governed by the Telecom Regulatory Authority of India, which regulates all telecommunication services in the country. Comprehensive data protection legislation applicable to all industry sectors is, however, currently being drafted. During this interim period, amendments have been proposed to the Indian Information Technology Act of 2004, which are intended to provide some privacy protections against information security breaches.

Indian law generally requires that information stored in electronic form be kept secure, but this requirement is imposed in the context of computer security rather than data protection. For example, section 43(a) of the Indian Information Technology Act includes provisions providing penalties for unauthorized access to a computer system. Section 43(b) of that law provides penalties for unauthorized downloading or copying of data. Section 72 creates an offense for accessing any electronic record, book, register, correspondence, document, or other material and disclosing such information without the consent of the person concerned.

Indian law does not yet impose specific obligations or liabilities on data processors. Several recent scandals in the Indian outsourcing industry have increased political pressure for such standards to be developed.

D. Japan

The Personal Information Protection Act ("PIPA") imposes overarching principles and requirements for data protection. PIPA became effective on April 1, 2005. PIPA applies to any business operating in Japan that possesses or has possessed personal information of more than 5,000 individuals, regardless of nationality, on any day in the past six months. Such an entity is considered a Business Handling Personal Information ("BHPI"). "Personal information" is defined as identifying information relating to a living individual. It includes name, date of birth, postal and e-mail address, phone number, job title, photograph, and employment-related information such as salary. In addition, it includes information that does not identify a specific individual when considered alone, but which could identify a specific individual when considered together with public information.

As a BHPI, an employer must specify, to the extent possible, the purpose of use of the personal information it retains. If the purpose of use changes, the subsequent purpose must be reasonably related to the originally stated purpose. A BHPI may use the personal information only to the extent necessary to achieve the purpose of use specified, unless exemptions apply. Further, the BHPI must acquire personal information in a lawful and fair manner, must promptly notify the individual concerned of the purpose of use or publicly announce the purpose of use unless it has already been publicly announced, and must respond to complaints from individuals, including by implementing a process to address complaints. PIPA requires BHPIs to keep personal data up-to-date and accurate, and mandates the adoption of security measures appropriate to prevent unauthorized disclosure, loss or destruction of personal data. PIPA further requires BHPIs to ensure that vendors and subcontractors handling personal information act in compliance with PIPA.

PIPA generally prohibits BHPIs from releasing personal data to third parties without the individual's consent, unless an exception applies, including when the disclosure is:

- made as part of an outsourcing arrangement;
- required or permitted by Japanese law;
- necessary to preserve life, safety or wealth, and it is difficult to obtain the individual's consent;
- necessary to improve public health or the sound upbringing of children, and it is difficult to obtain the individual's consent; or
- required of a business by a government body where obtaining consent of the individual concerned might impede the execution of government business.

Data processing need not be notified to any government authority under PIPA. Companies in the financial and telecommunications sectors are required to register or notify their business to their respective supervising authorities, the Financial Services Agency and the Ministry of Internal Affairs and Communications, respectively. Companies operating in these sectors are not required to specifically register their privacy practices unless the minister of the agency requests such registration.

The supervising minister investigates violations of PIPA and may order a BHPI to submit a report on its handling personal information or may issue a recommendation that the BHPI take appropriate steps to correct any breach of personal information. If such measures are urgently required, the supervising minister can issue an order requiring the BHPI to cease the violation and take corrective measures. If the BHPI does not comply with the order, it may be liable for a fine of not more than 300,000 yen (approximately \$2,500). Criminal penalties of up to six months are also possible. In addition to the charges under PIPA, organizations can be accused of defamation or an infringement of privacy through civil proceedings.

While PIPA is the main data protection legislation, Japan has also enacted sectoral guidelines and ordinances. Each Japanese ministry or agency issues guidelines that detail particular requirements for specific industries or specific types of information. For example, in the financial sector, the Financial Services Agency ("FSA") has published the Guidelines on Personal Information Protection for the Financial Sector, while the Ministry of Internal Affairs and Communications regulates the telecommunications sector via the Guidelines on Personal Information Protection for the Telecommunications Sector.

The FSA Guidelines have become an essential part of information security regulations, requiring that companies immediately report an information security breach to the supervisory authorities. Any company experiencing a breach must also: (1) notify the individuals whose information was breached; (2) publicize the facts of the breach; and (3) publicize its plan to prevent a recurrence and any secondary damage. The Guidelines do not distinguish between data that are subject to unauthorized access, such as hacking, and data that are lost or destroyed. It is not clear how promptly the requisite notices must be given, particularly if an investigation of the breach is ongoing.

The FSA has already initiated two enforcement actions under PIPA. On May 20, 2005, it issued a warning to a bank, requiring that the bank improve its information security measures, including employee supervision, following the loss of a CD-ROM containing personal information on 1.3 million corporate customers. The president of the bank was summoned to the Tohoku Local Finance Bureau to receive the warning personally, which was also issued to senior bank officials. The bank was required to rectify its data

management system and to improve supervision of its employees who have access to personal data. On April 25, 2006, a second enforcement action was initiated in which the FSA alleged negligence by bank management for failing to ensure sufficient information security. The charge stemmed from the discovery that a bank employee had accessed and sold sensitive customer financial information. Based on PIPA and the Banking Act, the FSA penalized bank management by reducing for two months the president's salary by 30 percent and the board's salary by 15-20 percent. Both incidents were widely reported in Japan and reportedly negatively impacted the banks' reputations.

E. People's Republic of China

China is currently considering and drafting data protection legislation. It is not yet clear whether the legislation will cover all industry sectors, and no draft has been made public. China also has not designated a data protection regulatory authority. The Ministry of Public Security, the Ministry of Information Industry, the Ministry of Culture and the Department of News and Publications may have some influence in this field. It is possible that a federal data protection authority will be established when the data protection legislation is enacted. Internet service providers are required to register some aspects of their data processing activities to the Ministry of Public Security under the Regulation on Internet Information Services of 2000, though this requirement is motivated by law enforcement concerns rather than data protection.

With regard to spam legislation, the Chinese Ministry of Information Industry's Measures for the Administration of Internet E-Services took effect on March 30, 2006. The Measures are primarily applicable to the transmission and receipt of unsolicited bulk commercial and advertising e-mails. Although certain aspects of the Measures are stated broadly, and although some matters (such as SMS spam delivered to mobile telephones) are left unresolved, the Measures essentially define the rights of e-mail users and the obligations of e-mail service providers. The Measures impose various restrictions on commercial e-mails for the purpose of limiting spam volume, including the following:

- a provider of Internet e-mail services must register the IP address of its Internet e-mail server with the Ministry of Information Industry;
- no organization or individual may send commercial advertisements e-mail without the recipient's clear consent;
- if a recipient has consented to receive commercial advertisements by e-mail but asks to stop receiving them, the sender must stop sending them;
- no organization or individual may intentionally conceal or forge Internet e-mail header information;
- no organization or individual may send commercial advertisement e-mail, without indicating in the subject line that the e-mail is an advertisement; and
- the sender of commercial advertisements e-mail must provide the recipient with a means of contacting the sender to refuse to continue receiving the e-mails.

The Measures also prohibit other e-mail-related activities, such as prohibiting the use of e-mail to produce, copy, publish and transmit information detrimental to the State or individuals' legal rights and interests, prohibiting the use of e-mail to endanger network safety or information safety, and prohibiting the use of other's computer systems to send e-mail without their authorization. The Measures also establish the

Center for Acceptance of Reports on Violative E-mails where individuals can file complaints regarding offending e-mails.

F. Singapore

There is no general data protection or privacy law in Singapore. The general proposition to adopt data protection legislation has been officially under review by the government for 13 years. For purposes of e-commerce, in 2002, the National Internet Advisory Committee proposed the Model Data Protection Code (“MDPC”) for the Private Sector, which was implemented by the National Trust Council in 2003. The MDPC is voluntary, providing standards for the collection and use of customer data by businesses that are certified by the National Trust Council.

In September 1998, the National Internet Advisory Board released an industry-based self-regulatory E-Commerce Code for the Protection of Personal Information and Communications of Consumers of Internet Commerce (the “Code”). The Code encourages providers to ensure the confidentiality of business records and personal information of users, including details of usage or transactions. It prohibits the disclosure of personal information, and requires providers not to intercept communications unless required by law. The Code limits information collection, prohibits the disclosure of personal information without informing consumers and providing an opportunity to object, ensures the accuracy of records, and provides a right for consumers to correct or request deletion of the data.

Development of anti-spam legislation was initiated in May 2004. The Info-Communications Development Authority (“IDA”) announced a multifaceted approach including legislation, public education and self-regulation of the marketing industry. The IDA and the Attorney General’s Chambers of Singapore issued a joint report proposing the legislative strategy for anti-spam legislation and recommended an opt-out approach. The report also recommends requiring advertisers to label marketing e-mail as such and prohibiting fake return e-mail addresses. Employer monitoring of employee phone calls, e-mails, and Internet usage is also permissible under Singapore law. Under Singapore property law, workplace e-mail, telephone and computer contents are the property of the employer. Thus, if an employee loses his job because of the contents of his communications technology, he has no grounds for defense based on an invasion of privacy.

Singapore’s Banking Act prohibits disclosure of financial information without the customer’s permission. In addition, the Monetary Authority of Singapore issued new “Know Your Customer” guidelines on money laundering to banks in May 1998. Banks are required to clarify the economic background and purpose of any transactions of which the form or amount appear unusual in relation to the customer, finance company or branch office concerned, or whenever the economic purpose and the legality of the transaction are not immediately evident. Banks must report suspicious transactions to the Monetary Authority.

G. South Korea

South Korea presently has a data protection regime similar to Japan, with one act covering the public sector and sectoral legislation for the private sector. In 2005, South Korea introduced the Personal Information Protection Act, which would have combined the existing sectoral statutes and created a Personal Information Protection Commission to oversee businesses maintaining databases of personal information. The Personal Information Protection Act has not been enacted.

The 1994 Act on the Protection of Personal Information Maintained by Public Agencies regulates automated processing of personal data in the public sector. This statute recommends that private entities respect the data protection principles set forth therein, but it lacks administrative or enforcement mechanisms to implement or enforce this recommendation. Acts governing the collection, use and disclosure of personal information in the private sector include the Protection of Communications Secrets Act (1993), the

Telecommunications Business Act (1991), the Medical Service Act (1973), the Real Name Financial Transactions and Secrecy Act (1997), the Use and Protection of Credit Information Act (1995), the Framework Act on Electronic Commerce (1999), the Digital Signatures Act (1999), and the Act on Promotion of Information and Communications Network Utilization and Data Protection (2000).

The Use and Protection of Credit Information Act of 1995 protects credit reports. In July 2001, three large credit card companies were fined under this law. The companies were found to have disclosed their customers' personal information (including bank account numbers, salary levels, and credit card transaction records, and customer identifiers such as names, addresses, phone numbers and resident-registration numbers) to insurance companies without giving notice to their customers or obtaining their consent in advance.

The Act on Promotion of Information and Communications Network Utilization and Data Protection (the "PICNUDP"), modeled after the German Online Service Data Protection Act of 1997, came into effect in 2000. The PICNUDP adopts common "fair information principles" and rules for the collection, use, and disclosure of personal data by "providers of information and communications services," such as common carriers, Internet service providers and other intermediaries, particularly content providers. The Act also covers specific offline service providers such as travel agencies, airlines, hotels, and educational institutes. Among other restrictions, the PICNUDP prohibits a "data user" from sending unsolicited commercial e-mail contrary to the recipient's explicit refusal of such e-mail. All unsolicited commercial e-mail must contain the word "Advertisement" in the subject line of every message and must contain opt-out instructions and contact information for the sender.

There is significant overlap between the aforementioned statute, the Framework Act on Electronic Commerce ("FAEC"), and the Digital Signatures Act ("DSA"). The FAEC requires data users to give data subjects sufficient information regarding the purpose of data collection. Under the FAEC, the data user must obtain explicit consent from the data subject before collecting personal information, and is prohibited from using the personal information collected for inconsistent purposes. Additional requirements of the FAEC include appropriate security and a right of access, correction or deletion. The DSA prohibits an individual from fraudulently using another person's private access passwords or other access key.

H. Thailand

Thailand is in the process of implementing the Privacy Data Protection Act, which is being jointly drafted by the Office of the Official Information Commission and the Ministry of Information and Communication Technology. It is not clear when the law might take effect. Other acts, such as the Official Information Act *BE* 2540 (A.D. 1997) (the "OIA") and the Credit Information Business Operation Act B.E. 2545 (A.D. 2002) (the "CBA") currently address privacy issues.

The OIA guarantees individual rights to have full access to government information. Under the OIA, almost all government-held data should be publicly available, with only a few categories of confidential information exempted from disclosure. The OIA provides individuals with the right to request access, inspect, and request copies of government-held information, to make complaints and appeals regarding their requests, and to ask the government to correct or revise information.

The CBA establishes rules for business operators, processors and controllers of credit information in order to ensure that their business operations will not violate the personal rights of consumers. In addition, the CBA prescribes the rights and obligations of entities that use services provided by credit reporting agencies and similar companies. Consumers also have the right to be informed of the identity of entities storing their credit information and the location of storage, as well as the right to correct their credit information.

The CBA provides for the appointment of the Credit Information Protection Committee, which has the power to supervise credit information businesses. Pursuant to the CBA, written consent must be obtained from the individual before a credit information business may disclose the individual's credit information to customers, although a few exceptions are provided. The CBA also requires credit information businesses and processors acting on their behalf to provide information security standards and systems that prevent misuse or unauthorized access to credit information.

Financial institutions or other members or customers of a credit information business must notify their customers within 30 days of providing credit information to the credit information business. The Credit Information Protection Committee has established criteria, procedures and conditions establishing the notifications that are due to customers when additional credit information, such as credit card payment histories, are provided to the credit information business.

Violations of the CBA are subject to civil penalties. For example, compensation may be due to individuals if a credit information business or processor dealing with credit information deliberately or negligently discloses inaccurate credit information to others. As a further example, failure to provide the requisite information security systems may result in a fine of up to Baht 300,000 (approximately \$8,000) together with a daily fine not exceeding Baht 10,000 (approximately \$267) for ongoing violations.

CANADA

Canada has two federal privacy laws, the Privacy Act and the Personal Information Protection and Electronic Documents Act ("PIPEDA"). In addition, the Federal Bank Act regulates the use of personal financial information by federally-regulated financial institutions.

The Privacy Act, in effect since July 1, 1983, regulates the privacy practices of federal government departments and agencies. The Privacy Act limits rights of collection, use and disclosure of personal information. It also gives individuals the right to access and correct the personal information about them held by federal government organizations. PIPEDA, enacted in 2000 and fully effective in 2004, sets rules for how private sector organizations may collect, use and disclose personal information in the course of commercial activities. A brief outline of PIPEDA, followed by a general discussion of provincial laws, is provided below.

A. Applicability

PIPEDA applies to all private sector organizations, including the retail sector, publishing companies, the service industry, manufacturers and other provincially-regulated organizations. PIPEDA does not apply to employee and workplace privacy in non-federally regulated organizations. The Act's privacy provisions apply to personal information that the organization collects, uses or discloses in the course of commercial activities. It also applies to personal information about employees of an organization that the organization "collects, uses or discloses in connection with the operation of a federal work, undertaking or business." PIPEDA defines personal information as "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization."

PIPEDA does not apply to organizations that operate solely within a provincial jurisdiction if that province has enacted a privacy law that has been designated as substantially similar to PIPEDA. To date, Alberta, British Columbia, and Quebec have enacted private sector privacy legislation that has received a substantially similar designation. Newfoundland and Labrador have passed legislation, but it is not yet in force. Ontario has several privacy laws that will be discussed in more detail below, but has not passed legislation substantially similar to PIPEDA. PIPEDA continues to apply to the federally-regulated private sector and to personal information in inter-provincial and international transactions by all organizations engaged in commercial activities.

Personal information is therefore subject to a patchwork of laws:

- If the organization is federally regulated, the data are subject to PIPEDA.
- If the organization has a unionized workforce, the union may have bargained for workplace privacy rights that can be enforced by labor arbitrators or Canadian courts.
- If the organization is not federally regulated and does not have a unionized workforce, it must then consider whether a provincial statute applies (presently limited to Alberta, British Columbia, and Quebec).
- If the organization is not located in a province with a privacy statute, it is not federally regulated, and it does not have unionized workforce, the employment information is not likely subject to statutory privacy compliance requirements.

PIPEDA has received an adequacy finding from the EU, so an entity's compliance with PIPEDA may serve as the legal basis for data transfers from the EU to Canada.

B. PIPEDA'S Requirements

Under PIPEDA, an organization must obtain an individual's consent, except in a few limited circumstances, before collecting, using or disclosing personal information and must use that information for a reasonable purpose. Disclosure is only permissible when done for the purpose for which the company has consent. PIPEDA gives individuals a right to access their information and request any relevant corrections. Organizations are also responsible for following these restrictions with respect to information they have transferred to third parties for data processing. The organization must use a contract or other means to ensure that the third party will provide a comparable level of data protection.

The heart of the legislation is the Canadian Standards Association Model Code for the Protection of Personal Information. PIPEDA codifies the Model Code in Schedule One. The remaining privacy provisions create a series of exceptions to the Model Code and establish an enforcement regime. The ten principles of fair information practices spelled out in the Model Code include:

- *Accountability:* An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.
- *Identifying Purposes:* The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
- *Consent:* The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate.
- *Limiting Collection:* The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
- *Limiting Use, Disclosure, and Retention:* Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the

individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

- *Accuracy:* Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is used.
- *Safeguards:* Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
- *Openness:* An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
- *Individual Access:* Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
- *Challenging Compliance:* An individual shall be able to address a challenge concerning compliance with the principles listed above to the designated individual or individuals accountable for the organization's compliance.

PIPEDA does not expressly restrict the transfer of data to other countries, but entities must comply with the principles regardless of where data are transferred or processed.

C. Investigation, Enforcement and Penalties

The Privacy Commissioner of Canada, or "PCC," enforces PIPEDA. The PCC enjoys a wide range of investigative powers, but does not have order-making power akin to that of a court. Its investigative powers allow the PCC to, among other things, enter the premises of an organization and converse in private with any person there and examine or obtain copies of records relevant to its investigation. The PCC also has the power to conduct an audit. The PCC may "on reasonable notice and at any reasonable time, audit the personal information management practices of an organization if the Commissioner has reasonable grounds to believe that the organization is contravening" certain provisions and recommendations provided by PIPEDA.

The PCC cannot levy penalties for violations of the law. If the PCC wishes to impose sanctions for violations of the law, it must apply for an order of the Federal Court of Canada. The Court may: (1) order an organization to correct its practices in order to comply with PIPEDA; (2) order an organization to publish a notice of any action taken or proposed to be taken to correct its practices; and (3) award damages to the complainant, including damages for any humiliation suffered. In addition to penalties imposed by the Court, the PCC may make public any aspect of the personal information management practices of an organization if it considers such publication to be in the public interest.

D. Ontario

Ontario is among the most active of Canada's provinces in its regulation of privacy issues. Ontario currently has three privacy laws: the Freedom of Information and Protection of Privacy Act; the Municipal Freedom of Information and Protection of Privacy Act; and the Personal Health Information Protection Act. The Freedom of Information and Protection of Privacy Act and the Municipal Freedom of Information and Protection of Privacy Act both allow individuals access to government-held information relating to them (at the provincial level and the municipal level). The Personal Health Information Protection Act, enacted in

2004, gives individuals access rights to their personal health information held by health information custodians. The law is intended to protect the confidentiality and security of personal health information by restricting the collection, use and disclosure of such information. The Personal Health Information Act also contains an information breach notification requirement, requiring health information custodians to notify individuals in the event their personal health information is breached. The statute has been deemed to meet national privacy standards, which exempts health service providers in Ontario from the requirements of federal privacy legislation.

LATIN AMERICA

Privacy rights in Latin America are founded on the concept of “habeas data,” a doctrine intended to safeguard the privacy, informational, and self-determination rights of individuals. These rights are considered fundamental and appear in most national constitutions.

A. Argentina

Argentina has received an adequacy finding from the EU with respect to international data transfers and follows the same basic principles with respect to data controllers, data processors and data processing, and the rights of data subjects. Argentina’s primary data protection law is the Personal Data Protection Act No. 25.326. The Act, enacted by the National Congress and applicable at the federal level, may also be applied by provincial governments via local regulations and provincial data protection authorities. To date, however, none of the Argentine provinces have exercised their authority to promulgate regulations or empower data protection authorities, though federal law expressly encourages application of the Act at the local level.

At the federal level, Decree No. 1558/01 facilitates application of the Act. The Decree provides for creation of a national Data Bank Registry, which is managed by the National Directorate of Personal Data Protection. Data controllers and data processors are required to file registrations detailing the type of data processed, the purposes of processing, the form in which data will be collected and updated, any cross-referencing of data, security measures, the retention period, the conditions under which data subjects may access their data, and any transfers or disclosures of the data. The registration is to be completed prior to the implementation of data processing.

The Personal Data Protection Act employs many of the same terms and concepts as the EU General Directive. “Personal data” are defined as “information of any kind referring to determined or determinable physical or juridical persons.” Argentina is also unique in that its definition of “data subjects” is expansive such that Argentine laws govern data about identifiable persons and data relating to legal entities. Argentina also employs similar concepts of data controllers, which own data, and data processors, though data processors are sometimes termed “data users.”

In addition, and also similar to the EU data protection scheme, data subjects have the right to request access to and updating of their data. Also like the EU, personal information may not be transferred to countries that do not provide for an “adequate” level of data protection in their national laws. Argentina has itself received an adequacy finding from the EU. Self-regulatory conduct codes and contractual provisions may be considered to provide an adequate level of protection where the recipient of the data is not located in a country that has been granted an adequacy finding by Argentina. If entities choose to create professional codes of conduct, they must register these with the National Directorate. Although the National Directorate has not issued any adequacy findings, many companies rely on the same legal bases that are available for data transfers out of the EU, including model clauses and consent of the data subjects.

Noncompliance with the Personal Data Protection Act may result in criminal penalties or fines. In addition, data subjects may pursue a *Habeas Data Action*, thereby requesting and compelling certain

information about, or changes to, their personal data. This judicial remedy is available when an entity has not responded to a data subject's request for access within ten calendar days or fails to rectify inaccurate data within five business days.

B. Chile

Chile was the first country in the region to supplement the constitutional right to privacy with a comprehensive data protection law. Law No. 19,628, known as the "Law for the Protection of Private Life," applies to virtually any type of information pertaining to individuals and employs terminology similar to the EU General Directive. The law generally provides that entities must process personal data in accordance with the fundamental rights granted to individuals under the Chilean Constitution. Data may only be processed for the purposes for which it was originally compiled. In addition, entities may not process personal data unless expressly authorized by law or by the written consent of the data subject. That consent may be withdrawn at any time, which right cannot be limited or restricted by contract.

Entities are obligated to maintain personal data in an accurate, complete and up-to-date form. Data subjects may request rectification of any incorrect, misleading or incomplete data, and may request the deletion of obsolete data or data for which there is no longer any legal basis to support its processing.

Chilean law does not establish a national data protection authority, so there is no registration requirement, nor does it restrict international data transfers, as do the EU and Argentine schemes. An entity transferring data to affiliated entities or data processors must, however, ensure that the data are kept confidential, that data are used in a manner consistent with the specific purpose for which they were collected, and that due care is exercised to protect the data. Disclosures to other third parties require the consent of the data subject, unless otherwise provided for by law.

Since there is no national data protection authority, data protection law in Chile is enforced by individuals through court actions. For example, fines may be imposed when an entity fails to respond, within two days, to a data subject's request for information or to modify or delete their personal information.

C. Mexico

Mexico's Constitution protects the right to privacy, including the confidentiality of correspondence, providing that "One's person, family, home, papers or possessions may not be molested, except by virtue of a written order by a proper authority, based on and motivated by legal proceedings Private communications are inviolable. The Law will provide a criminal sanction to any act that attempts against the freedom and privacy of private communications."

Mexico does not have comprehensive data protection legislation, but is currently considering data privacy legislation based on the Privacy Framework developed by the Data Privacy Subgroup of the Asia-Pacific Economic Cooperation ("APEC"). The APEC Privacy Framework is designed to protect individual interests without hindering economic development in APEC member countries, such as Mexico. The Framework consists of nine Information Privacy Principles:

- *Preventing harm:* Entities must focus protections on preventing harm and misuse.
- *Notice:* Individuals must be informed about entities' information practices, and that notice should be clear and easily accessible.
- *Collection limitation:* Entities should only collect data that is relevant to their purposes.

- *Uses of personal information:* Entities should only use data for purposes that are made known to data subjects, or purposes that are compatible with those purposes.
- *Choice:* When appropriate, entities are to provide a clear and accessible mechanism for individuals to exercise choices about the use and transfer of their data.
- *Integrity of personal information:* Information must be kept up-to-date and should be accurate and complete.
- *Security safeguards:* Safeguards should be appropriate to the information use and transfer, and should protect against unauthorized access, use, modification or disclosure of the information.
- *Access and correction:* Individuals should have the right to access and correct their information, but in appropriate circumstances.
- *Accountability:* Data controllers are accountable to comply with these principles, and must hold their data processors accountable for complying with the principles.

This approach, if adopted as legislation, would be less burdensome for companies than the Argentine and EU approaches, which tend to be overly bureaucratic. In the absence of comprehensive legislation, privacy issues in Mexico will continue to be governed by a myriad of sector-specific laws, including the following:

- The Federal Consumer Protection Law (*Ley Federal de Protección al Consumidor*), which governs commercial advertising messages. Such messages must include the company's name, address, phone number and e-mail address. If a service provider sends the message on behalf of the company, their contact information must also be included. Consumers are entitled to opt out of receiving such messages, and to object to the disclosure of their information. A federal body, the *Procuraduría*, is authorized to maintain a centralized list of consumers that have opted out of receiving commercial messages, but has not done so to date. Consumers are entitled to file complaints regarding commercial messages with the *Procuraduría* and fines ranging from 150-5,040 Pesos may result.
- The Law of Protection and Defense of the User of Financial Services (*Ley de Protección y Defensa Al Usuario de Servicios Financieros* or "LPDUSF") provides certain rights and protections for consumers of financial services. The statute also created and regulates the National Commission for the Protection and Defense of Users of Financial Services (*Comision Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros* or "CONDUSEF"), which is in charge of promoting, defending and advising upon the rights and interests of financial institution customers. The LPDUSF protects the disclosure of banking, fiduciary and securities information.
- The Geographic and Statistics Information Law (*Ley de Información Estadística y Geográfica*) gives individuals the right to have their geographic or statistical data rectified when incomplete, inaccurate or obsolete. Disclosures of census data provided by individuals or held by civil or administrative registries are limited, and individuals may lodge judicial complaints in the event such information is impermissibly disclosed.

AFRICA

At present, South Africa is the only African nation with extensive privacy legislation. No other African nation has considered enacting comprehensive privacy or data protection laws.

SOUTH AFRICA

The South African legislature has not yet promulgated any specific cross-sector data protection legislation. The South African Law Reform Commission (“the Commission”) published *Issue Paper 24 (Project 124): Privacy and Data Protection* (“the Issue Paper”). The Issue Paper proposes that general principles of data protection should be developed and incorporated into future privacy and data protection legislation. The Commission envisions a flexible approach that allows industries to develop their own codes of practice in accordance with the principles set out in the legislation. The Commission released for comment a draft Protection of Personal Information Bill in October 2005. The Commission is likely to publish its recommendations at the end of 2006. The recommendations will be presented to the Minister of Justice who will make the decision to introduce legislation in Parliament.

Currently, certain sector-specific laws contain provisions relevant to data protection. The Protection of Personal Information Bill, in its current form, is intended to replace the data protection provisions of these laws. Provided below is an overview of the current constitutional, contractual, and common law rights of privacy, as well as certain sector-specific data protection laws. As above, if South Africa enacts broad cross-sector data protection legislation, these laws may be superseded.

A. Common Law/Constitutional Right to Privacy

The *actio iniuriarum* has protected the common law right to privacy for many years. The right to privacy, including the right not to have the privacy of one’s communications infringed, is contained in Section 14 of the 1996 Constitution of the Republic of South Africa. Case law appears to lend support to the existence of a right to informational privacy (referred to in the EU as the right to “informational self-determination”) under the broad constitutional right to privacy. Constitutional rights may, however, be limited in terms of a law of general application.

B. Contractual Right to Privacy

Parties to a data exchange often enter into a contractual non-disclosure agreement. Typically, this agreement requires the data recipient to obtain consent from the disclosing party whenever the data will be transferred or disclosed other than as specified in the contract terms. It should be noted that, under South African common law, consent may be revoked at any time.

C. The Promotion of Access to Information Act, 2000 (“PAIA”)

The PAIA outlines procedures for individuals to request and for public or private entities to grant or deny access to their records. It allows entities to refuse access when granting it would constitute an unreasonable disclosure of personal information. The PAIA also requires entities to take reasonable steps to establish adequate and appropriate internal measures to provide for the correction of personal information they hold. Under the PAIA, personal information includes race, gender, age, physical or mental well being, religion, education or employment history, any identifying number assigned to the individual, and the personal views or preferences of the individual.

D. The Electronic Communications and Transactions Act, 2002 (“ECTA”)

Chapter VIII of the ECTA relates to the protection of personal information obtained during an electronic transaction (defined as a transaction of either a commercial or non-commercial nature that occurs by way of data messages). Section 51 contains a number of voluntary data protection principles, including that the data controller (defined as a person who electronically requests, collects or processes personal information of a data subject) must have the consent of the data subject to collect or store his or her personal information. Furthermore, the data controller may not request, process or store personal information other than that which is necessary for the lawful purpose for which the information is required. Without consent or unless required by law, the data controller may only use the information for the disclosed purpose. A data controller may voluntarily subscribe to these principles by recording its intention in an agreement with the data subject. However, if a data controller decides to adhere to the Section 51 principles, he or she must subscribe to all of them and not merely a portion.

E. The National Credit Act

The National Credit Act became law on June 1, 2006. It applies to the consumer credit sector, and contains data protection provisions in Part B of Chapter 4. Under the Act, any person who receives, compiles or retains any confidential information pertaining to a consumer or prospective consumer must protect the confidentiality of that information. The information may only be used or disclosed as permitted by law or as requested by the consumer. The Act also grants a person the right to be advised before a credit provider reports any adverse information to the credit bureau and, if requested, to receive a copy of the information. The Act also grants access and correction rights free of charge, once per year. In addition, any person who reported incorrect information to a registered credit bureau must pay the consumer’s cost of correcting that information.

The National Credit Act extends to any credit agreement or proposed credit agreement regardless of the location of the credit provider. In circumstances where the National Credit Act applies to a credit agreement, it continues to apply to that agreement even if a party to that agreement ceases to reside or have its principal office in South Africa. It applies in relation to every transaction, act or omission under that agreement, whether or not that transaction, act or omission occurs within or outside South Africa.

CONCLUSION

Any business contemplating overseas expansion must consider privacy and data protection requirements in the countries in which it plans to do business. The relevant laws and regulations are evolving rapidly. Businesses operating overseas would be well-advised to closely monitor the legal climate relating to data protection so as to remain in compliance with these complex and varied rules.

For additional information regarding privacy and data protection laws in the U.S. and abroad, please contact us.

Lisa J. Sotto
(212) 309-1223
lsotto@hunton.com

Elizabeth H. Johnson
(919) 899-3073
ehjohnson@hunton.com

Jörg Hladjk
+32 (0)2 643 58 28
jhladjk@hunton.com

Amanda Nichols McGovern
(202) 419-2001
amcgovern@hunton.com

© 2007 Hunton & Williams LLP. These materials have been prepared for informational purposes only and are not legal advice. This information is not intended to create an attorney-client or similar relationship. Please do not send us confidential information. Past successes cannot be an assurance of future success. Whether you need legal services and which lawyer you select are important decisions that should not be based solely upon these materials. Contact: Lisa J. Sotto, Hunton & Williams LLP, 200 Park Avenue, New York, New York 10166, (212) 309-1223 lsotto@hunton.com.

HUNTON &
WILLIAMS



**MORTGAGE
BANKERS
ASSOCIATION®**

Investing in communities

1919 Pennsylvania Avenue, NW
Washington, DC 20006-3404
www.mortgagebankers.org
(800) 793-6222