A SELECT SURVEY OF INTERNATIONAL DATA PRIVACY LAWS

Presented by Christine Nicholas to the ISB International Law Section, January 24, 2013

Virtually every company collects and processes electronic data relating to its employees, customers, suppliers or other third parties, some of which information is private and protected by relevant legal requirements -- such as employment records, insurance and medical records, bank records, school records, arrest records, social security and similar government-issued identification numbers, etc.

E-commerce cannot take place without the electronic transfer of data, much of it personally-identifying data. Clients with employees outside of the United States or otherwise doing business outside of the United States need to be aware of international data privacy laws that may affect the information a business collects concerning employees, customers, suppliers, contractors and others, and how it may use and must safeguard the information.

DATA PRIVACY LAWS FROM A SELECTION OF COUNTRIES

Canada

Canada’s constitution has long been held to protect from government access informational privacy where there is a reasonable expectation of privacy, including “‘core biographical information’ that reveals ‘intimate details’ about a person’s lifestyle and individual choices.” The privacy of personal information in Canada is protected in federal, provincial and territorial legislation, notably The Privacy Act of 1983, and the Personal Information Protection and Electronic Data Act of 2000. The Privacy Act regulates federal government institutions’ relationship with personal information, and the Personal Information Protection and Electronic Data Act (PIPEDA) regulates private sector organizations’ relationship with personal information. The purpose of PIPEDA was to promote electronic commerce by protecting personal information that is collected, used or disclosed in connection with the commercial relationship.

Author Bio: CHRISTINE E. NICHOLAS received her BBA in management, cum laude, from the University of Massachusetts in 1982 and received her law degree from the University of Idaho in 1985, where she was the Symposium Coordinator for the Idaho Law Review. Christine’s practice areas include business, finance, and real estate transactions. Christine has practiced in-house and in law firms, and served several terms on and is a former chair of the governing council for the Idaho State Bar Business and Corporate Law Section, and is the present chair of the Idaho State Bar International Law Section. She is the author of “Teach an Old UCC Dog New Tricks, An Overview of the U.N. Convention on the International Sale of Goods,” Business Law Today, Vol. 18, No. 1, Sept./Oct. 2008, for which she received a 2009 Burton Distinguished Writing Award for Legal Excellence.

These materials are designed to provide general information prepared by professionals in regard to the subject matter covered, and provided with the understanding that no legal, accounting, tax, or other professional services are being rendered hereby. These materials should not be utilized as a substitute for professional service in specific situations.

Christine can be reached at (208) 345-2000 or cen@moffatt.com.
In general, under PIPEDA, a company has to identify the purpose for which personal information is collected, limit the collection, use and disclosure to that pre-defined purpose, and obtain consent from the individual for any other collection, use or disclosure. Additionally, personal information is to be retained only as long as necessary to fulfill the purpose for which it was originally collected. Schedule 1 of PIPEDA sets forth a Model Code for the Protection of Personal Information, which requires compliance with ten “fair information practices,” summarized in a “fact sheet” issued by the Office of the Privacy Commissioner of Canada as follows:

1. **Accountability**: Appoint an individual (or individuals) to be responsible for your organization’s compliance; protect all personal information held by your organization or transferred to third party for processing; and develop and implement personal information policies and practices.

2. **Identifying purposes**: Your organization must identify the reasons for collecting personal information before or at the time of collection. Before or when any personal information is collected, identify why it is needed and how it will be used; document why the information is collected; inform the individual from whom the information is collected why it is needed; identify any new purpose for the information and obtain the individual’s consent before using it.

3. **Consent**: Inform the individual in a meaningful way of the purposes for the collection, use or disclosure of personal data; obtain the individual’s consent before or at the time of collection, as well as when a new use is identified.

4. **Limiting collection**: Do not collect personal information indiscriminately; do not deceive or mislead individuals about the reasons for collecting personal information.

5. **Limiting use, disclosure, and retention**: Use or disclose personal information only for the purpose for which it was collected, unless the individual consents, or the use or disclosure is authorized by the Act; keep personal information only as long as necessary to satisfy the purposes; put guidelines and procedures in place for retaining and destroying personal information; keep personal information used to make a decision about a person for a reasonable time period. This should allow the person to obtain the information after the decision and pursue redress; destroy, erase or render anonymous information that is no longer required for an identified purpose or a legal requirement.

6. **Accuracy**: Minimize the possibility of using incorrect information when making a decision about the individual or when disclosing information to third parties.

7. **Safeguards**: Protect personal information against loss or theft; safeguard the information from unauthorized access, disclosure, copying, use or modification; protect personal information regardless of the format in which it is held.
8. **Openness**: Inform your customers, clients and employees that you have policies and practices for the management of personal information; make these policies and practices understandable and easily available.

9. **Individual access**: When requested, inform individuals if you have any personal information about them; explain how it is or has been used and provide a list of any organizations to which it has been disclosed; give individuals access to their information; correct or amend any personal information if its accuracy and completeness is challenged and found to be deficient; provide a copy of the information requested, or reasons for not providing access, subject to exception set out in Section 9 of the Act; an organization should note any disagreement on the file and advise third parties where appropriate.

10. **Provide recourse**: Develop simple and easily accessible complaint procedures; inform complainants of avenues or recourse. These include your organization’s own complaint procedures, those of industry associations, regulatory bodies and the Privacy Commissioner of Canada; investigate all complaints received; take appropriate measures to correct information handling practices and policies.

(see https://www.priv.gc.ca/resource/fs-fi/02_05_d_16_e.asp). If the collecting business is a federally-regulated business, PIPEDA also applies to the personal information of its employees.

PIPEDA and certain provincial laws in British Columbia and Alberta require organizations to take reasonable steps to safeguard personal information in their custody or control from risks of unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction. A company collecting personal information from Canadians should develop procedures to protect collected personal information, to respond to inquiries and complaints from Canadians, and to identify and respond to a privacy breach.

**Mexico**

Like Canada, Mexico’s constitution guarantees a right to privacy. In 2010, Mexico enacted a Federal Law on the Protection of Personal Data Possessed by Private Persons. This is a law of “public order,” meaning that contract provisions to conflict with this law are unenforceable. The Federal Institute for Access to Information and Data Protection (IFAI) is charged with enforcing the law and issued regulations under the law.

The Law applies to personal data that are processed, transferred, or disposed by private persons or entities. “Personal data” includes any information pertaining to an identified or identifiable natural person.

More stringent provisions apply to the handling of sensitive data, that is, those data that pertain to the race or ethnicity, health, genetic information, religion, philosophical and moral beliefs, union membership, political opinions and sexual preference of an individual. Further, even though financial and economic data are not included in the definition of “sensitive data,” their processing requires the express consent of the data subject.
The entities that are subject to the Law are individuals or legal persons that process personal data, other than credit information companies. In addition, like most other countries’ data protection laws, the Law excludes from its scope individuals who collect, store, and use personal data for personal purposes.

The Law regulates the processing of personal data. The definition of the term “processing” encompasses a broad range of activities that include collection, use, disclosure, storage, access, management, transfer and disposal of personal data. Data collectors must collect and process personal data in a lawful manner. The data must be relevant, necessary, accurate, and updated for the purposes for which they were collected.

Data collectors may process personal data only for the purposes stated in their privacy notice unless the data subject consents to a new use of the data for a purpose that is not compatible with or analogous to the purpose that is set out in the privacy notice. Data collectors may keep the data only as long as necessary in order to fulfill the purposes for which the data were collected, and must delete any data that are no longer necessary for these purposes.

Data collectors are required to give data subjects a privacy notice that identifies, among other things, the entity that collects the data, what personal data are collected from them, the purposes of the collection and processing of their personal data and the proposed transfers of personal data. In addition, the notice must indicate the options and means that data subjects may use in order to control the use and disclosure of their personal data and the means by which they can exercise their rights of access, rectification, cancellation, or opposition.

The notice must be provided to the data subject when the data are collected, unless the data were not collected directly from the data subject. The notice can be in printed form, electronic form, or other format, but must be provided in the same format that is used to collect the data, unless prior notice was already given. Special provisions apply when personal data are collected through mobile phones or text messages.

Data collectors must have in place appropriate administrative, technical, and physical safeguards in order to ensure that personal data are protected from loss, damage, alteration, destruction, and unauthorized access or use. The safeguards must be at least as secure as those that the data controller uses to manage its own data. Further, data controllers must keep data in a manner that allows the prompt exercise of the data subjects’ rights. In the case of a breach of security, the Data Protection Law requires that the data subjects be notified of the breach if the breach significantly affects the concerned data subjects’ economic or moral rights. The Data Protection Law does not require that other entities or government agencies be notified as well.

The Data Protection Law requires data collectors to designate a data protection official within their organization. The data protection official will be responsible for processing data subject requests for access, and for promoting the personal data protection within the organization.

The Data Protection Law provides for significant fines (up to CA$1.2 million) for violations such as collecting or transferring personal data without the consent of the data subject where such consent is required, or collecting data in a misleading or fraudulent manner. If sensitive
data are involved, the penalties will be doubled. In the case of continued violations, an additional fine will be imposed.

In addition, the Data Protection Law provides for imprisonment from three months to three years for data controllers who, for profit, cause a security breach of the database in their custody. The processing of personal data by deception or by taking advantage of a data subject’s mistake or the mistake of an authorized person may be sanctioned by six months to five year prison terms if done for profit.

Violators may also be liable for the payment of damages to the affected individual to compensate for harms or damages to the individual’s property or rights that result from the lack of compliance with the obligations of the data controller or its subcontractors.

On the issue of cross-border transfers of personal data, the Data Protection Law makes the data exporter responsible for ensuring the protection of the data, and requires:

- The data collector must inform the data subjects of the proposed transfer, and the data subject must consent to the transfer;
- A data collector that intends to transfer personal data to a third party in another country, other than to a subcontractor, must identify the purposes for which the data are transferred to the third party, and must inform the third party of the restrictions that are set forth in the data controller’s privacy notice; and
- The third party that receives the data must assume the same obligations as those that apply to the data controller.

There are several exceptions where consent is not required. These exceptions include where the transfer is made to a subsidiary or affiliate, or to a parent company or an associated company that operates under the same processes and internal policies; and where the transfer is in the interest of the data subject in connection with a contract that has been, or is to be concluded between the data controller and a third party. Another exception allows for the cross border transfer of personal data when necessary for the maintenance or fulfilment of a legal relationship between the data subject and data collector.

**European Union Member States**

In 1995, the European Union passed a comprehensive data privacy law. Called the European Union Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (“Directive”), it requires each EU member state enact its own local law adopting the thrust of the Directive. Thus, the Directive is the blue-print for all European data privacy laws. However, in each European country, that country’s privacy statute will determine data privacy rights and responsibilities in that country.

Current EU member states are:
- Austria (1995)
- Belgium (1952)
- Bulgaria (2007)
- Cyprus (2004)
- Czech Republic (2004)
- Denmark (1973)
- Finland (1995)
- France (1952)
- Germany (1952)
- Greece (1981)
- Ireland (1973)
- Italy (1952)
- Luxembourg (1952)
- Malta (2004)
- Netherlands (1952)
- Poland (2004)
- Portugal (1986)
- Romania (2007)
- Slovakia (2004)
- Slovenia (2004)
- Spain (1986)
- Sweden (1995)
- United Kingdom (1973)

Countries that are on the road to EU membership:

**Acceding country**

- Croatia
  (I.e., signed the accession treaty and is awaiting ratification by all EU countries and Croatia; anticipated to become the 28th EU member country on July 1, 2013.)

**Candidate Countries:**

- Iceland
Potential candidates:

- Albania
- Bosnia and Herzegovina
- Kosovo

(I.e., countries that have not yet fulfilled the requirements for EU membership – essentially have not yet demonstrated that they have (i) stable institutions guaranteeing democracy, the rule of law, human rights and respect for and protection of minorities; (ii) a functioning market economy and the capacity to cope with competition and market forces in the EU; and (iii) the ability to take on and implement effectively the obligations of membership, including adherence to the aims of political, economic and monetary union.)
2. To protect EU citizens from an aggressive wave of data collection and distribution;

3. To harmonize privacy laws across EU member states.

In the EU, processing of personal data is illegal, unless done “fairly” and “lawfully” and for “legitimate” purposes. This requires that data controllers process personal data of EU citizens consistent with certain “data quality principles:”

a. Fairness – process data “fairly and lawfully.”

b. Specific Purpose – ensure that data are processed and stored only for specified and legitimate purposes and not further processed in a way that is incompatible with those purposes.

c. Restricted – ensure that data are accurate and kept up to date where necessary so that “every responsible step [is] taken to ensure” that errors are “erased or rectified.”

d. Destroyed when obsolete – maintain personal data “no longer than necessary” for the purpose for which the data were collected and processed.

e. Security – process the data with adequate security, requiring that the data controller implement “appropriate technical and organizational measures to protect personal data against . . . destruction or . . . loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network.”

f. Automated processing – decisions from data processing cannot be “based solely on automated processing of data” that “evaluates personal aspects”

Complying with the foregoing principles is not enough, however, as the Directive provides that all processing of personal data is illegal unless:

1. The data subject consents, OR

2. The processing is necessary (not just convenient) to accomplish one of the following five objectives: (a) perform a contract to which the data subject is a party, (b) comply with a law, (c) protect the data subject’s “vital interests,” (d) advance the “public interest” or facilitate the “exercise of official authority”, or (e) further the data controller’s “legitimate interests” without infringing the data subject’s “fundamental rights and freedoms.”

On top of the foregoing rules, there are extra rules under the Directive that apply to “sensitive” data, which is personal data that discloses “racial or ethnic origin, political opinions, religious and philosophical beliefs, trade-union membership and health or sex life.” Under the Directive,
processing of all sensitive data is prohibited, unless an “explicit consent” to such processing has been “freely given.”

The data controller must give a lot of disclosure to the data subject. Personal data cannot be processed in secret in the EU. EU data controllers must tell data subjects what information will be and has been collected, why it was collected, who collected it and who can access it. The data subject must have access to the data itself “without constraint at reasonable intervals and without excessive delay or expense.” The data subject can offer corrections to data the subject claims contains error or ask the data controller to purge the erroneous information. A data subject may object to data being processed for purposes of direct marketing and to be informed the first time personal data is disclosed to a third party. A US business used to processing consumer purchases via barcode scanners, selling customer lists, and restricting employee’s access to that employee’s personnel file may find adapting to the Directive challenging.

The Directive places tight limits on transmitting personal data outside Europe – including internal information about company customers and employees transmitted intra-company from a European subsidiary to US headquarters.

Europe sees the United States as a country that has failed to offer an adequate level of data protection allowing a transfer of personal data from Europe to the United States, and the Directive operated as a barrier for US-based multi-national companies’ headquarters that need data on their own European customers, suppliers and employees, impeding data transmission by interactive websites and company intranets, human resources information systems (PeopleSoft, Oracle and the like), customer and employee directories, customer reservations and support systems, routine mail and e-mail communications, and even telephone calls. After much political wrangling, where the EU Commission attempted to get the United States to enact a comprehensive data protection law like the Directive, the Europeans and Americans hammered out a “safe harbor” compromise, which the EU Commission adopted as a “special decision” (which does not require EU member-state ratification). Under this safe harbor, US data processors can receive personal data from Europe if they agree to treat the data as if it were still physically in Europe and subject to the Directive. Accordingly, a self-certifying US data receiver has to comply with the following:

1. Notice – the US entity must ensure that European data subjects are told why the US entity is processing their data, are given the US processors’ identity and contact information, are told about their right to limit use, disclosure and transmission of the data and how to exercise that right, all in clear, conspicuous language communicated as soon as they are asked to disclose information that will be sent to the US.

2. Choice – the US entity must give European data subjects a chance to opt out of having their personal information disclosed to an independent third party (as opposed to an agent) or used for some reason other than why originally collected. This opt out choice must be clear, conspicuous, readily available, and affordable, and the choice must remain open continuously. Additionally, Europeans affirmatively must opt in to safe harbor transfers of sensitive information (i.e., data about medical and health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union
membership and sex life). Exceptions to this opt in requirement for sensitive data exists if the processing is:

(a) In the vital interests of the data subject or another person;
(b) Necessary to establish legal claims or defenses;
(c) Carried out in the course of legitimate activities by a foundation, association or other nonprofit body in pursuit of political, philosophical, religious or trade union purposes and under the condition that the data not be disclosed to third parties without consent;
(d) Required to provide medical care or diagnosis;
(e) Necessary to carry out an organization’s employment law obligations; or
(f) Related to data manifestly made public by the individual.

3. Onward Transfer – the US entity wanting to transfer personal data on to some third-party agent in the United States or abroad must first verify that the third-party agent subscribes to safe harbor principles, is subject to the Directive or another adequacy finding, or signs a “written agreement” binding it to the level of privacy protections under the safe harbor. If the third party clears one of these hurdles, the safe harbor party gets a defense, even if the third party ends up violating safe harbor rules (unless the safe harbor party should have known of the problem but failed to take reasonable steps to fix it).

4. Security – a US safe harbor processor must take reasonable steps to protect personal data from loss, misuse, unauthorized access, disclosure, alteration and destruction.

5. Data Integrity – personal data on file must be limited to the purposes for which an organization intends to use it and processed data should be reliable for their intended use, accurate, complete, and current.

6. Access – European data subjects must be offered access to their personal information housed in the United States under safe harbor, and they must have a way to correct, amend, or delete inaccurate information. A safe harbor company can, however, charge a reasonable fee to cover the cost of providing access and can set reasonable limits on access. Under certain circumstances, a safe harbor company can deny a European data subject access to his own personal data transmitted to the United States under safe harbor (generally to avoid prejudice to confidentiality obligations, interference with law enforcement, litigation, or legal or professional privilege or obligation, or disclosure would interfere with important countervailing public interests).

7. Enforcement – safe harbor companies must build dispute resolution mechanisms offered to European data subjects who have grievances, in order to provide European data subjects with ready access to affordable procedures for safeguarding rights under safe
The two ways a safe harbor company can provide these qualifying mechanisms are to buy a prepackaged privacy enforcement program that incorporates the safe harbor principles or to submit to European data protection authorities that have dispute resolution mechanisms already in place.

Notwithstanding the foregoing cumbersome provisions, safe harbor status is easy to obtain by logging on to the Department of Commerce website and completing a one-page form, or sending a letter certifying that it has adequate procedures and protections. This self-certification merely needs to disclose:

- The name of organization, mailing address, e-mail address, and telephone and fax number;
- A description of how the organization will process personal data received from the EU; and
- A summary of EU personal data handling policies, including where the privacy policy is available for viewing, its effective date, the contact office for handling complaints and access requests, and which statutory body has jurisdiction to hear claims for unfair or deceptive practices and other legal violations (generally Federal Trade Commission or Department of Transportation), which privacy programs the organization subscribes to, what is the organization’s method of compliance verification (in-house or third party) and what independent body will investigate unresolved complaints. Thereafter, the organization needs to annually renew its safe harbor status with a short re-filing.

Safe harbor compliance causes the self-certifying company to be subject to regulatory review and enforcement of its procedures by the FTC, who reviews privacy violations as unfair and deceptive trade practices. (A small percentage of self-certifying companies are subject to DOT regulatory review and enforcement of their data privacy compliance). Financial institutions that fall outside the scope of FTC and DOT authority are not eligible to join the safe harbor program. Continuing to represent safe-harbor participation after having failed to renew will likely result in FTC enforcement action, as was recently the case with the “Safe Harbor Six” – 6 US businesses that allegedly falsely claimed they participated in the safe harbor program and were subject of FTC enforcement actions that resulted in settlements.

There are three alternatives to safe harbor compliance available to a US multi-national to solve compliance issues. The first is to obtain express consent from each individual providing personal data. The EU has issued an opinion that express consent from employees is not valid, as it was not “freely given.”

The second is to enter into contractual arrangements, the terms of which have been “pre-approved” by the European Commission. Acquisitions or other corporate changes may require new contracts, and the terms of the contracts cannot be changed without European Commission approval.
The third alternative is the concept of “binding corporate rules.” Multi-national organizations may comply with European data protection requirements through binding corporate rules approved by European data protection authorities in the relevant EU countries. With European data protection authority approval, an organization’s internal rules and procedures will satisfy local data protection obligations. Negotiating with multiple authorities takes time and discourages widespread use of this option.

A quick look at the export.gov safe harbor list (https://safeharbor.export.gov/list.aspx) shows more than 2500 US-based corporations self-certify to safe harbor compliance (including local businesses Micron Technology, Inc., URS Corporation, HP and certain of its specified subsidiaries, and ClickBank), making it the most popular compliance choice.

**China**

Data protection laws in China are unsurprisingly sparse. While the Chinese constitution indirectly refers to privacy rights in the home and for correspondence, China does not have sufficient legal infrastructure to protect individual privacy. The Law on the Protection of Minors does prohibit collecting “personal secrets” of minors. China has no internet-related data protection law and is recognized as the world leader in governmental monitoring and censoring of citizens’ internet use.

According to an internet posting by BakerHostetler on January 8, 2013, China’s top legislature, the Standing Committee of the National People’s Congress, closed out 2012 with the approval of rules to enhance the protection of online personal information. The “Decision of the Standing Committee of the National People’s Congress to Strengthen the Protection of Internet Data” (“Decision”) took effect upon its December 28, 2012, passage and was enacted “to protect network information security, protect the lawful interests of citizens, legal persons and other organizations, [and] safeguard national security and social order . . . .” Though the Decision’s primary purpose is to protect the personal online information of Chinese citizens, it includes an identity management policy requiring Internet users to use their real names to identify themselves to service providers, including internet or telecommunications operators.

The Decision reflects China’s recent push to address the issue of online personal data protection, and follows a Chinese Ministry of Industry and Information regulation, which took effect in March 2012, requiring Chinese websites to follow stricter rules on user consent to the collection and sharing of their personal data. Specific regulations regarding the protection of online data include the following:

- Internet service providers (ISPs), public service units (PSUs), and other organizations that collect or use an individual’s electronic information during business activities must clearly indicate the objectives, methods, and scope of collection and use of information and obtain consent for collection from the data subject.

- ISPs must strictly safeguard the privacy and strengthen the management of personal digital information.
Chinese citizens have the right to compel an ISP to delete personally identifying or private information about them or to take measures to terminate certain “harassing” activities.

ISPs are required to instantly stop the transmission of illegal information once it is spotted and take relevant measures, including removing the information and saving records, before reporting to supervisory authorities.

Organizations and individuals are banned from obtaining personal digital information via theft or other illegal means, and prohibited from selling or illegally providing the information to others.

“Supervising Departments” are empowered to take measures to prevent, stop, or punish those who infringe on online privacy, obtain personal digital information through illegal means, or sell or illegally provide information to others, and ISPs are required to give support during investigations.

Violators of the Decision rules are subject to liability including warnings, fines, confiscation of unlawful income, cancellation of permits or cancellation of fines, closure of websites, prohibition of relevant responsible personnel from future engagement in the network service business, and other civil, administrative and even criminal punishments. Violations may also be recorded in the “social credibility files” and be made public. The Decision looks more like a set of guiding principles than a law, and many of the provisions lack the specificity essential for accurate understanding and compliance. For example, there is no guidance regarding which governmental department or agency will supervise or enforce the rules.

Some privacy protection regulations in China have been passed at the local government level, most notably in the commerce center of Shanghai, which has enacted consumer protection rules that provide that a business is prohibited from disclosing a consumer’s personal information (name, gender, employment status, education, contact information, marital status, income, assets and health history) to third parties and cannot ask consumers to provide any personal information unrelated to the business at hand.

**Taiwan**

Protection of data privacy in Taiwan occurs chiefly under its constitutional freedom of privacy of correspondence and its 1995 Computer-Processed Personal Data Protection Act as amended in 2010 by the Personal Data Protection Act that became effective in October 2012 (“Data Protection Act”). Inspired by the EU Directive and Organization for Economic Cooperation and Development guidelines on data collection, the Data Protection Act prohibits anyone from collecting, processing or using Sensitive personal information except in narrow circumstances. “Sensitive personal information is defined as information related to medical treatment, genetic data, sex life, health examination, and prior criminal records, and may only be processed when (1) explicitly required by law, (2) necessary to carry out a statutory obligation, (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.
Non-sensitive personal information may be collected and processed only for a specific purpose when (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. Non-sensitive personal information may be used for a purpose different from why it was initially collected when (x) the information is expressly required by law, or (y) necessary to avoid danger to the life, body, freedom or property of the data subject, or (z) the written consent of the data subject has been obtained.

The data collector must give notice to the data subject when personal information is collected, and must include information such as the name of the entity that is collecting the data, the purposes of collection and use, the type of information to be collected, and the duration of use of the data. The data collector must also advise the data subject of its rights to access and correct the data. If personal information is not collected directly from the data subject, notice must be given to the data subject prior to processing or using the data, and the data subject must be advised about the source of the personal information being collected.

Consent must be in writing, and given only after any required notice.

Private-sector organizations that hold personal information must adopt appropriate security measures to prevent data from being stolen, altered, destroyed, eliminated or divulged, and must maintain the accuracy of the data, supplementing or correcting it on their own initiative or upon request of the data subject.

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

The Data Protection Act does not regulate off-shore data transmissions, such as to the United States, but allows government agencies the authority to restrict international transfers in the industries they regulate under certain circumstances, such as when (1) the transfer involves a major national interest, (2) there are special provisions in an international treaty or agreement restricting the transfer, (3) the receiving country does not yet have proper laws and regulations to protect personal data, and (4) personal data are indirectly transmitted to a third country to evade the Data Protection Act.

Under the original Data Protection Act, organizations collecting or processing data had to register and obtain a license. The Data Protection Act as amended abolished the license requirements, and there are no longer any obligations to file registration with any authority in order to collect personal data.

Upon the occurrence of a data breach, the data controller must complete an investigation of the circumstances of the breach and thereafter notify data subjects of the breach.
Violations of the Data Protection Act may result in five years in prison (versus two years before the recent amendment) or a fine of up to 1 million New Taiwan Dollars (presently equal to about US$34,000; versus NT$40,000 before the recent amendment).

**South Korea**

Korea’s constitution protects Koreans’ privacy at home and in correspondence. Statutes have been passed to implement those constitutional rights. Among them are the Electronic Transaction Basic Act, passed in 1999 to regulate e-commerce, and the Framework Act of Electronic Commerce and the Electronic Signature Act that regulates identity theft and regulates notifying data subjects of their data being processed and their rights of access to the data.

In late 2011, South Korea passed its Personal Information Protection Act, which went into enforcement March 31, 2012. I have not been able to locate an English translation of the Act, but reviewed other available materials discussing the Act. It has been described by commentators as the ‘strictest in the world’ and, therefore, the Asian law to which attention should be paid. The new Act replaces the existing Public Agency Data Protection Act in whole, and in relation to the private sector it replaces, in part, the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.

That Act will continue to provide additional privacy and other obligations on information and communications service providers. Korea’s previous legislation had considerable limitations. In the private sector, its scope was limited to businesses utilizing telecommunications services. It was actively enforced by a novel mediation structure that is being continued under the new legislation. The public sector legislation, administered by Ministry of Public Administration and Safety, covered all public agencies, and included most basic principles of the Organization for Economic Cooperation and Development, but with few limits on excessive data collection by governments. However, there seems to have been minimal enforcement. The new Act is a comprehensive Act covering both public and private sectors, and the whole of the private sector rather than only telecommunications businesses as under prior law. More than 3.5 million public entities and private businesses are now regulated by common criteria and principles, and common enforcement mechanisms.

The Act creates a 15-member Data Protection Commission. According to the Commission’s website, the objective of the Act is to “increase the people’s rights and to ensure the protection of the people’s dignity and values.” The underlying principles of the personal information protection afforded by the Act is to insure collected information is used for the goals specified when soliciting the collection, that only a minimum amount of information is collected and that it be accurate and safeguarded. The Act creates the Commission as an independent body under the President’s direct jurisdiction. The Act imposes liability to aggrieved persons for compensation for damage.

According to an article published in the June 2012 issue of Privacy Laws & Business International Report (available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2120983), the Act limits collection of personal data to the minimum needed for the purpose of collection, and requires that the data be processed in anonymity if possible. Under the Act, the data
A data collector must issue a privacy policy covering the Act’s requirements, must appoint a privacy officer, notify data suppliers of a data privacy breach (and in some circumstances notify regulatory authorities as well), and cannot export any data in violation of the Act and can only export after getting the data provider’s prior consent.

Data subjects may sue for damages for breach of any provision of the Act, and the burden of proof is on the data collector to show lack of “wrongful intent or negligence” and due care and supervision, as the case may be.

India

India is one of the world’s largest destinations for the outsourcing of processing of personal information through call centers and transcription of medical notes, but its data privacy laws are still being developed. Until recently, India lacked a true data privacy regime.

Like many countries, India’s constitution has been interpreted to include the protection of personal privacy rights (as an “essential ingredient of personal liberty”).

India’s Information Technology Act 2000, as amended in 2008, does not deal specifically with data protection and lacks core concepts of personal data, processing, disclosure and consent, and deals principally with electronic transactions and digital signatures.

In April 2011, India’s Ministry of Communications and Information Technology adopted rules under the Information Technology Act that purport to require a collector of “sensitive personal data” obtain consent from the data provider of the collection and usage of the data, and prohibit the collection of sensitive personal data unless it is collected for a lawful purpose connected with the collector’s function and its collection is necessary for that function. The information shall be used for the purpose for which it is collected and retained for only so long as is required for the purposes for which collected, and the data collector must permit the data providers, as and when requested, to review the supplied data and “ensure that any personal information or sensitive personal data or information found to be inaccurate or deficient shall be corrected or amended as feasible.” The data collector shall also, prior to collection, provide an option to the data provider not to provide the data and to withdraw its consent at any time “while availing the services or otherwise.”
Under the Rules, data collectors must keep the data “secure” and address grievances by the data provider through a Grievance Officer designated by the data collector, who shall redress grievances “expeditiously but within one month from the date of receipt of grievance.”

Disclosure of sensitive personal data to third parties requires prior permission from the data provider “unless such disclosure has been agreed to in the contract between the [data collector] and [the data provider], or where the disclosure is necessary for compliance of a legal obligation [including disclosure to government agencies for the purpose of verification of identity or for prevention, detection, investigation, prosecution and punishment of offenses].”

The information may be transferred to any corporation or person within or without India that ensure the same level of data protection required by the Rules, but only if “necessary for the performance of the lawful contract between the [data collector] and [the data provider] or where such person has consented to data transfer.”

Reasonable security for the protection of personal data includes the implementation of security practices and standards “commensurate with the information assets being protected with the nature of business,” such as pursuant to International Standard IS/ISO/IEC 27001 on “Information Technology – Security Techniques – Information Security Management System – Requirements.” Adoption of the foregoing standard is deemed compliance with the requirements of the Rules. If there is a security breach, the data collector has to demonstrate that it has implemented control measures pursuant to its documented information security program and policies.

In 2005, India adopted the Credit Information Companies (Regulation) Act, which contains a comprehensive set of data protection standards for credit information companies, though there is poor evidence that it has been enforced or complied with. It is regulated by the Reserve Bank of India.

The Rules define “personal information” as “any information that relates to a natural person which, either directly or indirectly, in combination with other information available or likely to be available with [a data collector] is capable of identifying such person.” “Sensitive personal data or information” means personal information that relates to:

- Password;
- Financial information such as bank account, credit or debit card or other payment details;
- Physical, physiological and mental health condition;
- Sexual orientation;
- Medical records and history; and
- Biometric information;

but excludes information freely available in the public domain.

The new Rules were designed to ensure that all personal information that a company collects is secure and obliges those who handle sensitive personal information to implement security practices and set up a dispute resolution process. The Rules have been initially viewed as more
restrictive than other countries’ data privacy laws because they do not exempt the service provider or vendors to the data collectors from these obligations, frustrating the purpose many companies have outsourced to or set up service companies in India. Many such companies are waiting to see how it will be implemented.

MANAGING DATA PRIVACY

A US company doing business in foreign jurisdictions needs to be mindful of the data privacy laws not only of the United States, but of the other countries where it does business, including countries where its collected data may be housed or accessed (for example, foreign countries where the US company has a subsidiary or operates on contracts for customer call-center). It may be desirable to have a single data privacy policy company-wide, rather than separate data privacy policies for each separate country operation. Therefore, it is good company practice to adopt a privacy policy that provides the basic framework for all data protection compliance activities that includes, among other things, guidance on the transfer of data outside the country, internet usage, and e-commerce. A privacy policy sends a clear signal that privacy law compliance is taken seriously and can help to demonstrate a company’s commitment to data protection. Any adoption of privacy policy must be properly communicated and supported by any necessary training to ensure that staff members are aware of the rules and understand them. Compliance with policy must be regularly monitored, and breaches sanctioned. Contracts with third-party delegates should be reviewed to ensure that they, too, contain provisions regarding the protection of personal data. Organizations should periodically undergo independent data security audits to analyze each of the company’s policies or, if the company has none, to promulgate a policy.

DEALING WITH A DATA SECURITY BREACH

The best time to deal with a data security breach is before a breach occurs by the adoption of a plan for responding to a data security breach. The plan should include setting up a security breach response team and developing and implementing a written data security response plan that sets out procedures to follow in the event of a data security breach that will satisfy the requirements of the jurisdictions where the company does business. Then, as soon as a data security breach is discovered, the company is prepared to take all necessary steps to investigate the incident promptly and to limit further data loss. With an appropriate response plan in place, a company will be able to timely comply with any applicable statutory notification requirements. For most practicable purposes, complying with applicable law after a data breach that affects employees or customers across a number of jurisdictions often means ascertaining and complying with the breach notification rules of the jurisdiction where the breach occurred and the home jurisdiction of each breach victim.

Data breaches can sometimes implicate notification requirements under other laws, such as financial disclosure laws. For example, where an HR data breach somehow leaks regulated information about publicly-traded securities (such as data about employee equity plans), securities laws might be implicated.
Resources:

List of data privacy laws from http://www.informationshield.com/intprivacylaws.html:

- **Argentina**: Personal Data Protection Act of 2000 (aka Habeas Data).
- **Australia**: Privacy Act of 1988.
- **Belgium**: Belgium Data Protection Law and Belgian Data Privacy Commission Privacy Blog.
- **Brazil**: Privacy currently governed by Article 5 of the 1988 Constitution.
- **Bulgaria**: The Bulgarian Personal Data Protection Act was adopted on December 21, 2001, and entered into force on January 1, 2002. More information at the Bulgarian Data Protection Authority.
- **Canada**: The Privacy Act - July 1983. Personal Information Protection and Electronic Data Act (PIPEDA) of 2000 (Bill C-6).
- **Chile**: Act on the Protection of Personal Data, August 1998.
- **Colombia**: Two laws affecting data privacy - Law 1266 of 2008 and Law 1273 of 2009. Also, the constitution provides any person the right to update their personal information.
- **Czech Republic**: Act on Protection of Personal Data (April 2000) No. 101.
- **Denmark**: Act on Processing of Personal Data, Act No. 429, May 2000.
- **Finland**: Act on the Amendment of the Personal Data Act (986) 2000.
- **Greece**: Law No. 2472 on the Protection of Individuals with Regard to the Processing of Personal Data, April 1997.
- **Hong Kong**: Personal Data Ordinance (The “Ordinance”).
- **Hungary**: Act LXIII of 1992 on the Protection of Personal Data and the Publicity of Data of Public Interests (excerpts in English).
- **Iceland**: Act of Protection of Individual; Processing Personal Data (Jan 2000).
- **Ireland**: Data Protection (Amendment) Act, Number 6 of 2003.
- **India**: Information Technology Act of 2000.
- **Japan**: Personal Information Protection Law (Act) (Official English Translation) Law Summary from Jonesday Publishing.
- **Korea**: Act on Personal Information Protection of Public Agencies Act on Information and Communication Network Usage.
- **Lithuania**: Law on Legal Protection of Personal Data (June 1996).
- Morocco: Data Protection Act.
- Norway: Personal Data Act (April 2000) - Act of 14 April 2000 No. 31 Relating to the Processing of Personal Data (Personal Data Act).
- Philippines: DATA PRIVACY ACT OF 2011. There is also a recognized right of privacy in civil law and a model data protection code.
- Romania: Law No. 677/2001 for the Protection of Persons concerning the Processing of Personal Data and the Free Circulation of Such Data.
- Poland: Act of the Protection of Personal Data (August 1997).
- Portugal: Act on the Protection of Personal Data (Law 67/98 of 26 October).
- Singapore - The E-commerce Code for the Protection of Personal Information and Communications of Consumers of Internet Commerce.
- Slovak Republic: Act No. 428 of 3 July 2002 on Personal Data Protection.
- Slovenia: Personal Data Protection Act, RS No. 55/99.
- Spain: ORGANIC LAW 15/1999 of 13 December on the Protection of Personal Data
- Taiwan: Computer Processed Personal Data Protection Law (applies only to public institutions).
- Thailand: Official Information Act, B.E. 2540 (1997) for state agencies. (Personal Data Protection bill has been under consideration for years.)
  Privacy and Electronic Communications (EC Directive) Regulations 2003 official text, and a consumer oriented site at the Information Commissioner’s Office.

United States laws with data privacy provisions include:

- Americans with Disabilities Act, 42 USC § 12101, *et seq.*
- Cable Communications Act of 1984, Pub. L. 98-549
- California Civil Codes 1798.29, 1798.82 and 1798.84 (as amended by California Senate Bill 1386).
- Electronic Funds Transfer Act (EFTA), 15 USC § 1693, *et seq.*
- Driver’s Privacy Protection Act of 1994, 18 USC §§ 2721-2725.
- Family Education Rights and Privacy Act of 1974 (FERPA), 20 USC § 1232g.
- Privacy Act of 1974, 5 USC § 522a.
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. 107-56.

For data privacy laws in Asia, see http://privacyasia.blogspot.com/p/privacy-and-data-protection-legislation.html