Tips for Coping with Global Data Privacy Regimes

Nick D'Ambrosio[1], JD, Director, KPMG LLP

Up-to-date overview, by country: rules and regulations on data privacy and blocking statutes
Tips to establish data integrity protocols for gathering, transporting and storing data across borders

[1] The opinions expressed herein the author's and may not reflect those of KPMG LLP. The information provided relates to generalized compliance and investigation issues and recommendations, but is not intended to be a substitute for informed and qualified legal counsel.

Contents

I. Conducting Corporate Investigation Without Trampling on Data Privacy Rights

An analogy to the "Fog of War" may not be overstatement with regard to some high stakes regulatory-related corporate investigation such as those addressing allegations of price fixing, Foreign Corrupt Practices Act or antimony laundering violations. The consequence can be grave – harm to the company's reputation, large civil and criminal fines, and possible imprisonment for the guilty. As compliance professional and investigators we are trained to get to the truth by securing and safeguarding data, scanning computer hard-drives, securing email and file back-ups and processing and mining what inevitably includes an employee's personal data.

As a result, data privacy rights are often a secondary concern and, if addressed at all, are often remembered too late. This presentation provides compliance professionals with an overview of the comprehensive "cradle to grave" data privacy regimes such as the European Union Data Protection Directive as well as country specific requirements including the United States and many of the 89[2] countries that have adopted data privacy laws and regulations. Local employment or labor law may also impact employee's data privacy right; however, this presentation does not address these issues.

II. Protected Information

According to Pillbury Winthrop Shaw Pittman LLP:

> As a rule, only personally identifiable information ("Personal Data") is afforded special protection by data privacy laws. This usually includes one or more types of data that identifies or is linked to an identifiable living individual (e.g., name or Social Security Number). In some cases, it includes a combination of such information that could potentially identify an individual (e.g., birth date, gender and postal code taken together). Many (but not all) data privacy laws exempt Personal Data that has been encrypted. Certain types of "Sensitive Data" are often given enhanced protection under comprehensive data protection regimes. Sensitive Data may include, for example, race, ethnicity or national origin, political opinions or associations, union membership, sexual orientation, marital status, health-related information and criminal history. It should be noted that data privacy laws are not restricted to protecting active employee information, so companies' obligations extend to any non-employee groups whose Personal Data they may acquire, such as clients and customers, but also job applicants, consultants, independent contractors and terminated or retired employees (Source, www.pillsburylaw.com, "Employee Data Privacy—An Overview of Employer Responsibilities, October 20, 2011, retrieved 18 Feb 2013).

A. U.S. and Global Employee Data Privacy Laws

Corporate investigations often span international boundaries and invariably touch upon employee data in increasing forms and volumes. Because the United States does not have a comprehensive policy on employee data privacy law, American investigators are often surprised to learn that more than 89 countries have laws and regulations protecting data privacy. The paper presents a broad overview of

[2] Greenleaf, Graham, *Global data privacy laws: 89 countries, and accelerating*. Privacy Laws & Business International Reports, Issue 115 Special Supplement, February 2012. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000034 retrieved on 18 Feb 2013.

global data privacy and blocking statutes with a focus on how the internal corporate investigator can establish a protocol for the lawful gathering, processing, transportation and storage of employee data.

III. U.S. Federal Privacy and Data Protection Laws

A. Federal Constitutional Law

The United States Constitution does not generally apply to monitoring conducted by private companies, but rather only employee monitoring conducted by federal, state, or local government agencies.

In the absence of a comprehensive legal framework for privacy and data protection, the U.S. has in place a mixture of legislation, regulation and self-regulation. As a result, the regulations cover a wide range of very specific personal information rights, for example financial information, video rental and vehicle registrations. The U.S. privacy regulation takes two tacks: 1) protection from federal government and 2) private sector industry-specific protection (healthcare information, banking and finance information).

At the time of this writing, the Federal Energy Regulatory Commission (FERC), the independent agency that regulates the interstate transmission of natural gas, oil, and electricity, and also regulates natural gas and hydropower projects, does not have a data privacy policy or regulation (McAfee.com retrieved 18 Feb 2013).

B. Electronic Communications Privacy Act

The Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act are commonly referred together as the Electronic Communications Privacy Act of 1986 (ECPA). The ECPA updated the Federal Wiretap Act of 1968. The older Wiretap Act had been written to address interception of conversations using "hard" telephone lines. The onset of computer and other digital and electronic communications prompted the need to make the update. Generally, 'electronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic or photo-optical system that affects interstate or foreign commerce.

Title I of the ECPA protects wire, oral, and electronic communications *while in transit*. It sets down requirements for search warrants that are more stringent than in other settings. Title II of the ECPA, the Stored Communications Act (SCA), protects communications held in electronic storage, most notably messages *stored on computers*. Its protections are weaker than those of Title I, however, and do not impose heightened standards for warrants. Title III prohibits the use of pen register and/or traps and trace *devices to record dialing, routing, addressing, and signaling information* used in the process of transmitting wire or electronic communications without a court order.

The USA PATRIOT Act and subsequent federal enactments have clarified and updated the ECPA in light of the ongoing development of modern communications technologies and methods, including easing restrictions on law enforcement access to stored communications in some cases.

> **Sidebar:** Email stored on a third party's server for more than 180 days is considered by the law deemed abandoned, and all that is required to obtain the content of the emails by a law enforcement agency, is a written statement certifying that the information is relevant to an investigation, with absolutely no judicial review required whatsoever.

> When the law was initially passed, emails were stored on a third party's server for only a short period of time, just long enough to facilitate transfer of email to the consumer's email client, which was generally located on their personal or work computer. Now, with online email services prevalent such as Gmail and Hotmail, users are more likely to store emails online indefinitely, rather than to only keep them for less than 180 days. If the same emails were stored on the user's personal computer, it would require the police to obtain a warrant first for seizure of their contents, regardless of their age. When they are stored on an internet server however, no warrant is needed, starting 180 days after receipt of the message, under the law. (Source: Wikipedia, "Electronic Communication Privacy Act" retrieved 19 Feb 2013.)

Among the exceptions under the EPCA, there are three which would relieve an employer from liability for monitoring its employees' e-mails: (1) consent (which includes implied consent), (2) the "provider" exception (which applies when a company provides its own e-mail service or communications systems), and (3) the "intra company communications" exception (when the employer accesses stored communication files).

1. Consent

The ECPA allows employers to intercept electronic communications if the employee consents in advance. To remove the expectation of privacy by employees, employers should establish a formal Internet Acceptable Use Policy (IAUP) that puts an employee on written notice that any electronic non-business-related activities are done at the employee's own risk and can by monitored by the employer, and that password protection is not an indication of personal privacy.

2. "Provider" Exception

The Privacy Rights Clearinghouse observed that,

In a June 2010 decision, *City of Ontario v. Quon*, the Supreme Court unanimously upheld the search of a police officer's personal messages on a government-owned pager, saying it did not violate his constitutional rights. The warrantless search was not an unreasonable violation of the officer's 4th Amendment rights because it was motivated by legitimate work-related purposes. The city was trying to determine whether it needed to modify its wireless contract, which imposed fees after employees exceeded character limits on text messages.

The city obtained a transcript of Quon's messages during an investigation to determine whether officers were using their pagers for personal messages. The transcripts showed that Quon had been exchanging sexually explicit messages. The Court's decision generally allows government employers to look at workers' electronic messages if employers have reasonable, work-related grounds.

The privacy issue in *City of Ontario v. Quon* involved a government intrusion into personal communications, that is, whether or not the 4th Amendment applied to the electronic communications of public employees. The 4th Amendment would not apply to a private employer. However, the decision could have an impact on future court decisions involving private employers.

There is one important lesson to be had from the *Quon* case: An employer's policy regarding monitoring need not specify every means of communication subject to the policy. As an employee, you should assume that any electronic device provided by an employer may be subject to monitoring, whether or not such a device is specifically mentioned in a written policy (www.privacyrights.org retrieved 18 Feb 2013).

One employment law counsel summarized the import of the *Quon* decision to private employers as follows:

The Court then proceeded to issue its decision based upon the assumption that the supervisor's statements overrode the department's policies and did allow the officer to have a reasonable expectation of privacy in his text messages. This quasi-ruling by the Supreme Court may give employers some heartburn, because it seems to indicate that even a good, effective company policy may be overridden by a passing comment by a supervisor. Ouch!

On the other hand, the Supreme Court's ultimate ruling will likely be helpful to employers. It held that "because the search was motivated by a legitimate work-related purpose, and because it was not excessive in scope, the search was reasonable," for purposes of the Fourth Amendment claim. While the Court was careful and narrow in the rationale behind its ruling regarding the expectation of privacy, it went out of its way to broaden its ultimate holding to include the private employer context, stating, "the Court also concludes that the search would be 'regarded as reasonable and normal in the private-employer context....” 130 S. Ct at 2633 (emphasis added).

Therefore, for private employers, the *Quon* decision teaches:

- An employer's computer-usage and e-mail policies can be expanded to cover other applications, such as text messages, by follow-up clarifications and memoranda
- The computer-usage and e-mail policy can remove any reasonable expectation of privacy by the employee
- Passing comments by a supervisor may reinstate the reasonable expectation of privacy
- But monitoring of the e-mails, text messages and the like by a private employer may still be regarded as "reasonable," so long as it was (a) motivated by a legitimate work-related purpose, and (b) not excessive in scope (http://www.lypelaw.com retrieved 18 Feb 2013).

3. Web-Based Personal Email and Other Accounts

There are few reported cases addressing the monitoring of employee's personal web-mail accounts by an employer.

In *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, Inc.* (S.D.N.Y., decided December 22, 2010), a gym owner filed suit against his former employees for setting up a competing business. The former employees had signed non-compete agreements. The employer filed a suit using as evidence 546 e-mails from the employees' Hotmail and GMail accounts which showed that the employees had taken customer lists and training materials, as well as solicited customers. This access was obtained because the former employees had used the “auto-stored” feature for user-name and password fields which were accessible to the employer when he logged on to his employees accounts. The former employees countersued claiming that the employers’ access of their personal email accounts was a violation of the Stored Communications Act of the EPCA. The Court found that the employer had violated the law by this unauthorized access. The former employees argued that all 546 emails that were accessed constituted separate violations of the statute entitling them to $1,000 per violation in statutory damages. The Court instead found that due to the closeness in time between the accesses of the personal email accounts, they collectively constituted only one violation for the purpose of damages.

C. General U.S. Employee Privacy Guidance

It is generally well-settled than an employer may monitor an employee's use of company-provided e-mail systems, smart phones, internet usage, and the like. The key consideration for the employer is to have a clear, clearly communicated policy which removes any reasonable expectation of privacy from the employee in connection with such use of company equipment or accounts, whether that use occurs at work or away from work. Far less settled is the issue of monitoring employee's mixed business and personal use of employee-purchased devices such as smart phones, tablets, etc.

IV. European Union Data Protection Laws

The EU Data Protection Directive, adopted in 1995, requires the counties within the EU to enact comprehensive data protection laws. The "Eight Principles" of the Directive establish the minimum standards for these national laws. These principles govern the "processing" of "personal data." The term "processing" includes virtually everything that can be done with data – collection, recording, disclosure, dissemination, making available, combination, blocking, erasure, and destruction of data. The term "personal data" means any information that (a) relates to a natural person; (b) identifies that person, either on its own or in combination with other information (such as a table of employee identification numbers) that is in the organization's possession or that is likely to come into its possession; and (c) is stored in an electronic file or manual filing system.

A. The Eight Principles

In accordance with the Eight Principles, "personal data must be:

1. Processed fairly and lawfully
2. Processed only for specific, limited purposes and not any manner inconsistent with those purposes
3. Adequate, relevant and not excessive in relation to those purposes
4. Accurate, complete and kept up-to-date
5. Kept in personally identifiable form no longer than necessary
6. Processed in accordance with the rights of the data subject under applicable law
7. Kept secure; and
8. Only transferred to countries that have "adequate" data protection laws unless the "data exporter" takes certain specific steps to ensure that the data is "adequately protected."

B. Restrictions on the Transfer of Data to Countries Outside the EEA

The general rule is that the EU Directive prohibits the "export" of "personal data" to countries outside of the EU, unless:

- The receiving country has adopted laws that, in the opinion of the European Commission (EC) , provide "adequate protection" for personal data
- One of several very limited exceptions applies; or

- The data exporter has taken steps to ensure to the satisfaction of the local data protection authorities that the data will be "adequately protected" after it leaves the EEA

C. Countries with "Adequate" Data Protection Laws

Personal data may be freely transferred to or among EEA countries and non-EEA countries that have been determined by the EC to have "adequate" data protection laws. The EC maintains a list of these countries (Permitted Countries).

To date, only Switzerland, Guernsey, Argentina, Isle of Man, Faroe Islands, Jersey, Andorra, Israel and New Zealand have been approved in full. Canada has been approved for certain types of personal data. According to the EC, the United States is not deemed to have "adequate" data protection laws.

> **Sidebar:** Therefore, if an EU subsidiary of a U.S. multinational plans to transfer data to its U.S. parent corporation for any purpose including an internal investigation, the subsidiary must first ensure local data protection authorities that one of three alternative means has been complied with to assure "adequate" data protection.

D. Alternative Means of Providing Adequate Protection

Personal data may not be exported from the EEA to an unapproved country unless the data exporter has followed procedures to ensure to the satisfaction of the local data protection authorities that the data will be "adequately protected" after it leaves the EEA.

The relevant country data protection authority with jurisdiction over "adequate protection" issues is where the data exporter is established and that authority establishes the standard for determining adequacy.

The data protection laws of a number of EEA countries (e.g., Spain) require the data exporter to

- Notify the data protection authorities before transferring personal data to a country that does not provide "adequate protection;" and
- Obtain a formal ruling that the data comes under one of the general exceptions or that the data exporter has taken appropriate steps to ensure "adequate protection."

  The laws of other countries (e.g., the U.K.) adopt a "proceed at your own risk" approach. While the data exporter is not required to obtain approval in advance, sanctions may be imposed if the data protection authorities later determine (usually in the context of a complaint) that the data exporter did not take appropriate steps to ensure adequate protection.

E. Exceptions to the Restrictions on Transfer

To provide some degree of certainty and predictability, the EC has issued Decisions that require the data protection authorities in each of the Member States to approve:

- Transfers to U.S. entities that have joined the U.S. Safe Harbor;
- Transfers made pursuant to a TBDFA agreement that incorporates Set I or Set II model clauses published by the European Commission; or
- All entities within the group of companies have entered into a global code of data protection conduct, generally referred to in the EU as Binding Corporate Rules or "BCR."

An in-depth discussion of the EU Data Protection Directive is beyond the scope of this overview. In particular, the process of joining and complying with U.S. Safe Harbor program and the BCR as well as the drafting of TBDFA agreements are matters for legal counsel. An excellent discussion of these issues is provided by Robert Bond, Esq., SpeechlyBircham, *Data Protection Laws: Resolutions and solutions to transfer of personal data within the European Union and from the European Economic Area to other countries*; http://www.globalcompliance.com/pdf/data-protection-laws-restrictions.pdf retrieved 18 Feb 2013.

1. U.S. Safe Harbor Program

The EU and the U.S. Department of Commerce have created a self-certification safe harbor program to whereby U.S. companies can certify their adherence to seven principles in order to become eligible to receive Personal Data from EEA nations. While the Safe Harbor program was intended to cover all personal data, in practice many U.S. companies have expressly limited their participation to certain types of data, such as human resource data. The U.S. Department of Commerce maintains a public list of Safe Harbor organizations at http://export.gov/safeharbor.

To comply with the Seven Principles a company must inform individuals:

1. What data is being collected
2. For what purpose the data is being collected
3. How the data will be used
4. How to contact the organization with inquiries or complaints
5. The types of third parties to which the data may be disclosed
6. The choices and means the organization offers individuals for limiting its use and disclosure, and
7. How data will be secured.

Before joining the Safe Harbor, a company must:

- Develop and implement a Safe Harbor Privacy Statement based on the Safe Harbor Principles
- Make its Safe Harbor Privacy Statement public
- Designate a “data protection” officer
- Establish an employee training program
- Establish a verification mechanism to audit the company’s compliance with Safe Harbor Principles; and
- Establish an independent dispute resolution mechanism.

The company must offer individuals the opportunity to choose whether their personal data may be:

- Disclosed to a third party; or

- Used for a purpose that is "not compatible" with the purposes for which it was originally collected or to which the individual subsequently consented.

While an "opt-out" mechanism satisfies this requirement in some circumstances, if the data is "sensitive" (i.e. specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual) then an affirmative "opt-in" is required.

The enforcement principles underlying the Safe Harbor program include the participating company's self-regulation and enforcement backed up as needed by Federal Trade Commission. The FTC's enforcement and sanctions are based on unfair and deceptive trade practices statutes. The FTC has both administrative and judicial enforcement powers to sanction companies for failure to adhere to Safe Harbor requirements.

2. Transborder Data Flow Agreement (TBDFA)

The EU Directives provide that the "adequacy" requirement may be met by "appropriate contractual clauses." There is a lack of consistency among Member State data protection authorities as to just what constitutes "appropriate contractual clauses."

V. Guide to Global Data Privacy Laws

Several leading international law firms compile country specific data privacy reference guides for their clients and the public. Because of the general format of these guides, it must be understood that they are not a comprehensive summary of all the issues that may be applicable to your company's specific circumstances and that you must seek qualified legal guidance before you act upon this information. Nevertheless, the presentation that follows is excerpted from three recent reference guides: 1) Norton Rose LLP's, *Global Data Privacy Director* issued February 2012 (http://www.nortonrose.com/files/global-data-privacy-directory-52687.pdf retrieved 18 Feb 2013); 2) DL Piper LLP, *Data Protection Laws of the World* issued March 2012 (http://www.dlapiper.com/data-protection-laws-of-the-world-handbook-03-01-2012/ retrieved 18 Feb 2013); and 3) U.S. Department of Commerce's, *International Data Protection Legislation Matrix* issued 2005 (http://web.ita.doc.gov/ITI/itiHome.nsf/51a29d31d11b7ebd85256cc600599b80/4947d6deb021a96485256d48006403af?OpenDocument retrieved 18 Feb 2013).

A. Europe and Russia

1. France

General: A comprehensive legislative regime arising from the implementation of the EU Data Protection Directive. Depending on the nature of the data processed and/or of the purpose of the processing, personal data may not be processed under the French DPA without giving prior notice to, and/or obtaining prior approval from, the Commission Nationale de l'Informatique et des Libertés (the CNIL).

Applicable legislation: French Data Protection Act n°78-17 of 6 January 1978 (amended) on data processing, data files and individual liberties (the French DPA).

Restrictions on transfer of data offshore: No restrictions on export to EEA countries or other Permitted Countries. Export to US entities covered by the US Safe Harbor privacy regime is permitted. Otherwise, transfer of data offshore is subject to restrictions (such as consent, EU model clauses, CNIL's prior authorization etc.).

Employers must do the following:

- collect the data for a specific purpose;
- hold the data only as long as needed;
- keep the data accurate and up to date;
- inform the employees why the data is being processed;
- inform the employees of any third parties that will be receiving the data;
- keep the data secure and confidential; and
- give employees access to the data and a chance to correct any mistakes.

2. Germany

General: A detail set of rules consistent with and following the principles of the EU Data Protection Directive. In general, prohibit the collection, processing and use of personal data unless permitted by law or with the explicit consent of the person concerned.

Applicable legislation: Germany is said to be the jurisdiction that globally enacted the first data protection act ever in the year 1970. Currently, the main law for the protection of personal data is the Federal Data Protection Act from 1990, which has been amended several times since. Major reforms have been enacted in 2003 and 2009.

Restrictions on transfer of data offshore: No restrictions on export to EEA countries or other Permitted Countries. Any export of personal data outside of the EEA implies a transfer to a third party which generally requires justification (irrespective of where the recipient is located). In other words, the transfer to a third party requires to be justified in the first place. That means, it is required that either a statutory provision allows for the transfer or the data subject has consented. According to German data protection laws these restrictions to transfers of data to third parties even apply with regard to data transfers within a group of companies. Germany has approved a standard contract for out-of-country transfers that does not require employee consent. For transfer of data to the United States, compliance with the US/EU Safe Harbor principles satisfies the requirements of Germany's transfer law.

Employers must do the following:

- collect the data for a specific purpose;
- hold the data only as long as needed;
- keep the data accurate and up to date;
- inform the employees why the data is being processed;
- inform the employees of any third parties that will be receiving the data;
- keep the data secure and confidential; and
- give employees access to the data and a chance to correct any mistakes.

3. Spain

General: Spain has developed general data privacy legislation broadly consistent with the principles in the EU Data Protection Directive. These rules apply to the processing of any personal data either by public or private entities.

Applicable legislation: A member of the European Union, Spain implemented the EU Data Protection Directive 95/46/EC with the 1999 Data Protection Act (the Act). The Spanish Data Protection Authority is very active and publishes a large number of Legal Reports and resolutions which, together with the rulings from Judges and Courts, set the basis for the interpretation of the above legislation.

Restrictions on transfer of data offshore: No restrictions on export to EEA countries or other Permitted Countries. Export to US entities covered by the US Safe Harbor privacy regime is permitted. There are several exemptions permitting an international transfer without obtaining the authorization from the Director of the Spanish Data Protection Authority, for example, obtaining of the free and unequivocal consent from every individual concerned. However these exemptions are interpreted restrictively by the Spanish Data Protection Authority. In any case, notification to the Spanish Data Protection Authority is required.

Employers must do the following:

- collect the data for a specific purpose;
- hold the data only as long as needed;
- keep the data accurate and up to date;
- inform the employees why the data is being processed;
- inform the employees of any third parties that will be receiving the data;
- keep the data secure and confidential; and
- give employees access to the data and a chance to correct any mistakes.

4. United Kingdom

General: The United Kingdom has a comprehensive legislative regime that implements the EU Data Protection Directive.

Applicable legislation: England and Wales has implemented the EU Data Protection Directive and the EU Directive on Privacy and Electronic Communications through the Data Protection Act 1998 and the Privacy and Electronic Communications (EC Directive) Regulations 2003 respectively. Scotland and Northern Ireland are separate legal systems to England and Wales but have almost identical legislation to that in place in England and Wales. The UK Information Commissioner is the regulator for all three jurisdictions. The UK Information Commissioner has powers to issue civil monetary penalties of up to £500,000 for non-compliance with the Data Protection Act.

Restrictions on transfer of data offshore: No restrictions on export to EEA countries or other Permitted Countries. Export to US entities covered by the US Safe Harbor privacy regime is permitted. There are several exemptions permitting an international transfer without obtaining the authorization from the Director of the Spanish Data Protection Authority, for example, obtaining of the free and unequivocal consent from every individual concerned. However these exemptions

are interpreted restrictively by the Spanish Data Protection Authority. In any case, notification to the Spanish Data Protection Authority is required.

Employers must do the following:

- collect the data for a specific purpose;
- hold the data only as long as needed;
- keep the data accurate and up to date;
- inform the employees why the data is being processed;
- inform the employees of any third parties that will be receiving the data;
- keep the data secure and confidential; and
- give employees access to the data and a chance to correct any mistakes.

5. Russia

General: Russia's Personal Data Law regulates the processing of personal data by public bodies and private entities.

Applicable legislation: In general, in Russia protection of personal data is subject to regulation by the Federal Law No. 152-FZ of 27 July 2006 "On Personal Data" (the Personal Data Law).

Restrictions on transfer of data offshore: The Personal Data Law introduces a procedure for the transfer of personal data by a personal data operator across the Russian state border to a foreign public authority, individual or legal entity. The transfer of data outside of Russia does not require additional consent from the relevant individual if the jurisdiction that the personal data is transferred to also requires adequate protection of personal data. In particular, the Personal Data Law allows such transfer of personal data to countries outside Russia that are parties to the European Council's "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data."

B. The Americas

6. Argentina

General: Argentina has in place federal personal data protection laws, which are consistent with the EU Data Protection Directive.

Applicable legislation: Data protection is governed by the following laws in Argentina: (a) Law No. 25,326 (Personal Data Protection Act); (b) Decree No. 1558/2001; and (c) Resolution No. 2/2005 issued by the National Office of Personal Data Protection. The main purpose of the Data Protection Act is to protect data stored in public or private databases, in order to guarantee personal honor, privacy and access to the data. The decree and resolution regulate the Personal Data Protection Act.

Restrictions on transfer of data offshore: The Data Protection Act prohibits the transfer of data to countries or international organizations that do not provide enough levels of protection to the data. However, decree 1558/2001 authorizes such transfer in the case of express consent granted by the data subject.

Employers processing personal data must provide clear advance notice to employees including:

- why the data is being collected;
- the name or category of anyone who will be receiving the data;
- that the relevant file exists, who holds it and where the holder is domiciled; and
- that the employees or their heirs, successors or assignees have the right to access, amend and delete the data.

Employers must:

- issue a statement confirming that the collected data is not excessive in light of its purpose, will not be used for any other from its stated purpose, is accessible to employees, is accurate, and can be updated;
- supply any information an employee requests about his personal data, and amend, update or suppress the data when appropriate; and
- treat employees' personal data as privileged, and take all necessary steps to ensure it remains secure and confidential.

7. Brazil

General: No law specifically refers to collecting, processing or transferring personal information about individual employees. However, privacy rights exist under Brazil's Constitution, Consumer Code, Habeas Data Law and Banking Secrecy Law.

Restrictions on transfer of data offshore: In general, Brazil's Constitution mandates employee consent to the transfer of the employee's personal data to a third party. However, transfer out of the country of some kinds of personal data within an economic group (to a subsidiary, parent or affiliate, for example) should be possible without employee consent, under the theory that labor legislation makes companies in the same economic group jointly liable.

8. Canada

General: In Canada, federal and provincial laws govern the collection, use and disclosure of personal information in the private sector. These laws are based on 10 fair information principles and strict controls over commercial electronic messages. These principles are consistent with the principles in the EU Data Protection Directive.

Applicable legislation: The Canadian Personal Information and Electronic Documents Act (PIEDA) federally regulates the collection, processing and transfer of personal information about individuals. In addition, a number of provinces, including Alberta, British Columbia and Quebec, have their own legislation on private sector data privacy. In Quebec, data privacy is regulated by the Act Respecting the Protection of Personal Information in the Private Sector (Quebec Privacy Act). Companies and activities subject to the Quebec Privacy Act are exempt from PIEDA for actions inside Quebec, according to the federal government.

Restrictions on transfer of data offshore: PIEDA allows the transfer of personal data out of the country when any of the following conditions are met:

- the employee consents;
- the transfer is necessary or required by law;
- the transfer is needed to protect the employee's vital interests; or
- the data comes from a public register.

For transfer of data to the United States, compliance with the US/EU Safe Harbor principles equals compliance with PIEDA.

Under PIEDA, an employer is required to:

- be answerable for its data privacy policies and practices;
- tell employees how it manages personal data;
- keep personal data accurate, complete and up to date;
- take proper security safeguards;
- provide employees with access to their personal data so they can correct or change it; and
- provide employees with recourse procedures they can use.

Under the Quebec Privacy Act, an employer holding, using or communicating personal data is required to:

- tell employees why it is collecting their personal data, how the data will be used, who will have access to it, and where the file will be kept;
- make sure employees understand their rights to see and correct the data;
- take proper security safeguards;
- make sure the data is accurate when it is used; and • obtain employee consent in some cases.

9. Mexico

General: Mexico has recently enacted a Data Protection Law (and corresponding Regulations) broadly consistent with international data protection principles. These rules apply to the processing (collection, use, disclosure or storage) of personal data by private entities.

Applicable legislation: Federal Law on Protection of Personal Information in Possession of Private Parties (Ley Federal de Protección de Datos Personales en Posesión de los Particulares) (hereinafter the "Data Protection Law") and its Regulations. The Mexican Data protection authority is the Federal Institute for Access to Public Information and Data Protection (Instituto Federal de Acceso a la Información y Protección de Datos) that has the authority to investigate compliance and sanction infringements to the Data Protection Law by both governmental agencies and private parties.

Restrictions on transfer of data offshore: None.

10. Venezuela

General: Venezuela Law does not have any specific regulatory framework for data protection. There is, however, general legislation applicable which provides for the protection of right to privacy and individual's personal data.

Applicable legislation: Venezuela does not have a general privacy law but there are provisions dealing with privacy rights in various laws, including: the Telecommunications' Privacy Protection Law; the Defense of Access to Goods and Services Law; the Data Messages and Electronic Signatures Law; the Special Law on Computer Crimes; and the Labor Working Environment and Working Conditions Law.

C. Asia-Pacific

11. Australia

Applicable legislation: Data protection in Australia is currently a mix of Federal and State/Territory legislation. The Federal Privacy Act 1988 (Cth) and its National Privacy Principles ("Privacy Act") applies to private sector businesses and its Information Privacy Principles apply to all Commonwealth Government and Australian Capital Territory Government agencies. Australian States and territories (except for Western Australia and South Australia) each have their own data protection legislation applying to State Government agencies (and private businesses interaction with them).

Restrictions on transfer of data offshore: Personal information may only be transferred outside of Australia or to a different organization (including a parent company) where:

- the organization reasonably believes that the information is subject to a law, binding scheme or contract which effectively provides for no less protection than the Privacy Act;
- 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;
- where the transfer is for the benefit of the individual, it is impractical to obtain their consent and if it were practical, they would be likely to give their consent; or
- where the organization has taken reasonable steps to ensure that the information will not be held, used or disclosed inconsistently with the Privacy Act.

12. China

Applicable legislation: Provisions relating to personal data protection are found in various laws and regulations, but none of the provisions clearly define the scope of privacy rights. The main provisions are found in the General Principles of Civil Law and the Tort Liability Law, which define such rights as a right of reputation or right of privacy. A draft Personal Data Protection Law has been under review by the government for many years, but there is still no indication as to if and when such law will be passed.

Recently, the Ministry of Information and Industry of China ("MIIT") published draft guidelines called the Information Security Technology – Guide for Personal Information Protection ("Draft Guidelines"). If the Draft Guidelines are eventually enacted, they would be likely to have a significant impact on how personal data is required to be handled.

Restrictions on transfer of data offshore: The Protection of State Secrets Law also regulates the disclosure and transfer of information that falls within the definition of state secrets. No current restriction, subject to any national security issues.

Proposed restrictions under the Draft Guidelines Data controllers may transfer personal data to third parties (group companies are considered third parties) if the following conditions are met:

- the data controller explains the purpose and subject of the data transfer to the data subject;
- the data subject explicitly consents to such transfer; and
- the data controller ensures the receiver has the capability to properly process the personal data and that the personal data will be safe during the transfer.

13. Hong Kong

Applicable legislation: The Personal Data (Privacy) Ordinance (Cap. 486) ("Ordinance") regulates the collection and handling of personal data. Enforcement is through the Office of the Privacy Commissioner for Personal Data ("PCPD"). A major amendment to the Ordinance is on the way.
Restrictions on transfer of data offshore: Data users may not transfer personal data to third parties, unless the data subjects have been informed of the following before their personal data was collected:

- that their personal data may be transferred; and
- the classes of persons to whom the data may be transferred.

There are currently no restrictions for transfer of personal data outside of Hong Kong. Although such restrictions are set out in the Ordinance, they are currently not in force.

14. India

Applicable legislation: The Personal Data (Privacy) Ordinance (Cap. 486) ("Ordinance") regulates the collection and handling of personal data. Enforcement is through the Office of the Privacy Commissioner for Personal Data ("PCPD"). A major amendment to the Ordinance is on the way.

Restrictions on transfer of data offshore: a corporate entity or any person acting on its behalf may transfer sensitive personal data to any other entity, either in India or abroad, if the recipient maintains the same levels of security as itself. The contract regulating the data transfer should contain adequate indemnity provisions for a third party breach, the end purposes of the data processing should be clearly specified (including who has access to such data) and the mode of transfer is adequately secured and safe.

D. Africa

15. Angola

Applicable legislation: Angolan law does not have any specific regulatory framework for data protection. There is, however, general legislation applicable which provides for the protection of privacy and personal data.

Restrictions on transfer of data offshore: There are no express restrictions on offshore transfers of data.

16. Nigeria

Applicable legislation: The Constitution gives every citizen the right to privacy.

Restrictions on transfer of data offshore: There is currently no legislation that prevents the transfer of data offshore.

17. South Africa

General: Venezuela Law does not have any specific regulatory framework for data protection. There is, however, general legislation applicable which provides for the protection of right to privacy and individual's personal data.

Applicable legislation: Although there is currently no data protection legislation in force:

- the Constitution of the Republic of South Africa guarantees the right to privacy;
- the Protection of Personal Information Bill ("PPI Bill"), when passed as law (not passed as of January 2013) will safeguard personal information by imposing stringent obligations on persons holding and processing personal information.

Restrictions on transfer of data offshore: Although there is currently no regulation of the transfer of data, this will be altered by the PPI Bill once passed as law.

E. Middle East

18. Israel

Applicable legislation: Israel has enacted the Protection of Privacy Law, 1981 (the "Privacy Law") in 1981.

Restrictions on transfer of data offshore: The transfer outside of Israel of data from a database in Israel is regulated by the Protection of Privacy Regulations (The Transfer of Information to a Database Outside the State Borders), 2001 (the "Regulations").

The Regulations prohibit the transfer of information from a database in Israel to a database located abroad, unless the receiving country in question ensures a level of protection of information which is not lower than the level of protection provided for under Israeli law.

19. Saudi Arabia

Applicable legislation: There is no specific law dealing with privacy and personal data in Saudi Arabia. Instead, there are provisions contained in various pieces of legislation (and industry circulars) that should be considered depending on the circumstances. Privacy is in general safeguarded under the Basic Law which is derived from the Shari'ah ("Islamic Code").

Restrictions on transfer of data offshore: Not applicable

20. United Arab Emirates

Applicable legislation: There is no specific data protection legislation in place at a Federal level in the United Arab Emirates ("UAE").

Restrictions on transfer of data offshore: According to the Penal Code (Clause 379), personal data may be transferred to third parties inside and/or outside of the UAE if the data subjects have consented in writing to such transfer. The requirement to obtain the written consent may be waived, pursuant to the Penal Code (Article 377) and Clause 3 of the Privacy of Consumer Information Policy, where:

- a UAE official/public authority has required the transfer of such data to it; and
- the transfer serves public interests or national security.

VI. Corporate Investigations of Possible Wrongdoing

A. Investigative Exceptions that Overtake the General Privacy Rules

The EU Directives and some national privacy laws relax the application of their privacy principles when to apply them would prevent an organization from advancing or defending itself against legal claims or undermining an investigation or prosecution of a criminal offense, including those occurring in the workplace. A number of EU Directive Articles address this exception:

- Article 8: Enables an organization to process investigative data related to an individual's commission of a criminal offense (i.e. "sensitive" personal data) where necessary for the "establishment, exercise or defense of legal claims" or "carrying out the obligations and specific rights of the controller in the field of employment law;"
- Article 13: Allows Member State's waiver of privacy rules related to notice and access when the personal data is being processed for the "prevention, investigation, detection and prosecution of criminal offenses, or the beach of ethics for regulated professionals;" and
- Article 26: Allows for otherwise prohibited transfers of personal data outside the EU "for the establishment, exercise or defense of legal claims."

The nature of these possible exceptions to employee privacy right with regard to corporate investigations, points out the careful balancing of competing legal rights that are in play. If the investigation is merely a "fishing expedition" with indiscriminate collection and review of personal data in the form of emails and other stored document no exception to employee data privacy rights will be justified. Similarly, if the investigation relates to possible serious criminal offenses such as price fixing, money laundering, accounting fraud, or bribery of government officials the case of an exception is more persuasive than if the issue is related to possible breaches of internal company policies.

B. Pro-Active Monitoring

In order to monitor employee activities to detect or prevent potential wrongdoing a company will be required to adopt clear and detailed corporate policies that inform the workforce of the company's monitoring policies with respect to email, Internet and other communication systems. Other discretionary notices to consider might be automatic pop-ups and warnings that appear on-screen to employees informing them that their communications may be monitored.

Recommended data privacy protocol for monitoring:

- Fair and lawful processing: ensuring the workforce and potential third-parties interacting with them are apprised of the company's monitoring;
- Proportionate processing: monitoring efforts are proportionate response under the circumstances and does not unjustifiably intrude on employee privacy;
    - Preference for sporadic rather than to continuous monitoring; review of high-level or aggregate data rather than individualized data; review of redacted or anonymized data rather than personal data; targeted rather than blanket surveillance; review of traffic data rather than communication content; review of business-related data rather than non-business data.
- Limited purpose: irrelevant data to the investigative purpose must be promptly deleted or destroyed and not used for another purpose;
- Security: monitoring data is stored with adequate security measures and that third party providers are subject to comparable security measures; and
- Data transfer: compliance with applicable restriction to transfer of data offshore.

C. Corporate Investigations

Recommended data privacy protocol for corporate investigations:

- Fair and lawful processing: The investigation cannot be conducted fully covertly as employees will need to act on investigation/litigation holds and hand over computer equipment, files for scanning. Therefore, the issue is one of when to notify employees of their data privacy rights and what to disclose. Employee policy statements that personal data may be processed by the company for "investigative purposes" or "to protect the company's interests" may not be sufficient to address data privacy regulator's concerns. If third parties such as computer forensic, external legal and/or accounting advisors will be involved in gathering and reviewing data, the notice should address these disclosures and seek the full cooperation of employees in the efforts. A separate written notice should be provided prior to data collection to each impacted employee to be returned with a signed acknowledgement receipt. Efforts should be undertaken to keep the identities of employees subject to the document review as confidential as practicable to avoid potential employee reputational damage. Guidance regarding notification of third parties (e.g. business contacts in a subject employee's Outlook address listing) is sparse, but companies generally rely on the EU Directorate's "disproportionate effort" exemption.
- Proportionate processing: Along with relevant data, collection efforts will confront plainly personal emails and files (e.g. music, photos). To avoid disproportionate data collection problems, efforts should be made prior to scanning employee hard-drives or server files to

copy only work-related and not personal files. However, most email, spreadsheet, word processing files will need to be read, at least in part, to ascertain whether they contain relevant information. When both relevant and irrelevant data is contained efforts should be made to redact as much irrelevant personal information as possible.

It may be prudent, if not required, to provide employees with access to their computers prior to scanning to exclude purportedly personal files from production. Further, proportionate processing requires that the time period under review be narrowly defined to address a reasonable investigative scope.

- Limited purpose: Irrelevant data to the investigative purpose must be promptly deleted or destroyed and not used for another purpose.
- Security: Investigative data should be stored with adequate security measures and that third party providers are subject to comparable security measures. Virtual data rooms should have limited controlled access based on unique IDs and passwords to authorized users; be audited to prevent or detect security breaches; and allow access to data on a read-only basis.
- Request for Access to Data: If a subject of an investigation request assess to his or her private data, unless such request is patently abusive, assess should generally be granted. Deadlines for granting access vary widely from with 10 to 40 days of request. However, the company's rights to effectively secure evidence of wrongdoing without giving the suspect an opportunity to erase or destroy potentially incriminating evidence is generally recognized as a legitimate exception or factor in granting access.
- Data transfer: Often the simplest, if labor intensive, process for complying with off-shore transfer prohibition is to redact or anonymize all indentifying information prior to transfer.

  A conundrum can arise when the U.S. parent company's investigation is related to violations of U.S. laws but not necessarily domestic laws of the country where the affiliate's data resides. For example, is French affiliate of a U.S. company obtains data related to French employees actions regarding possible FCPA violations, the general exemption related to "prevention, investigation, detection and prosecution of criminal offenses" will probably not be deem applicable by the French privacy regulators and transfer to the U.S. will not be permitted. A similar difficulty may also arise where the investigation is pursuant to a U.S. regulators' (i.e. FTC, SEC or Department of Justice) subpoena or court order to collect and disclose personal information. In an effort to curtail perceived concern that U.S. courts are extending U.S.-style discovery obligations to the international setting, countries including the United Kingdom, France, Sweden, and the Netherlands have enacted blocking statutes that prohibit disclosure of information of an economic, commercial, industrial, financial or technical nature to foreign public authorities. To date, only French law has substantial scope and attempts at enforcement.

D. Post-Investigation Finality Requirement

In general data gathered during monitoring or a corporate investigation should only be retained for as long as the any underlying legal proceedings are in progress and for some period thereafter in order to respond to any appeals. If no legal proceedings were brought, the period of retention should be no greater than the applicable statute of limitations.

Under most data privacy regimes, including the EU Directives, strict limitations are imposed on the use of collected personal data for unrelated commercial purposes of any sort. Therefore, companies must limit their use of the personal data and take steps to destroy the information as soon as practicable.