GLOBAL EQUITY DESK REFERENCE – DATA PRIVACY

ABOUT DLA PIPER

DLA Piper is a global legal services organization with 3,500 lawyers in 67 offices in 29 countries across Europe, North America, the Middle East, and Asia. The firm has established practices in corporate, tax, securities, human resources, employment, litigation, technology, and communications. DLA Piper's clients range from multinational, Global 1000, and Fortune 500 enterprises to emerging companies developing industry-leading technologies.

Only DLA Piper has more than 1,300 lawyers on each side of the Atlantic. Our unmatched global presence enables us to meet the ongoing needs of our clients in the world's key economic, technology, and government centers.

GLOBAL DESK REFERENCE

We hope that you find the information in this Desk Reference useful.

You should be aware that the information provided in the Desk Reference is presented in a general format and is not a comprehensive summary of all the issues that may be applicable to your company's specific circumstances. Furthermore, data privacy laws and regulations are constantly changing. These changes may not be incorporated into this version of the Desk Reference. With these factors in mind, it is important that you do not consider this Desk Reference to be legal advice and do not rely solely on the information provided. We would be pleased to help you review all pertinent information and can assist you in developing a comprehensive privacy strategy globally.

FOR MORE INFORMATION

If you have any questions about data privacy in any country, please contact:

DEAN FEALK
T: +1 415 836 2521
F: +1 415 659 7421
dean.fealk@dlapiper.com

DLA Piper LLP (US)
555 Mission Street, Suite 2400
San Francisco, CA 94105

© 2009 DLA Piper LLP (US)
GLOBAL DATA PRIVACY REGULATION

As companies collect and use personal, identifiable information about individual employees, conflicts may arise over the employees’ right to keep their personal information confidential. Many countries have enacted data privacy laws to control how information is collected, processed and shared; these laws impact a wide variety of company activities, including recruitment, payroll, work performance evaluations, employee benefits, disciplinary actions and company directories. Multinational companies, particularly those that manage human resources or other personnel functions in a central location and transfer information between countries, are increasingly challenged to conform their activities to a wide variety of data privacy laws.

Unlike the United States, which has no comprehensive data privacy law, Western European countries have a history of enacting strict data privacy legislation. Beginning in the early 1970s, France and other European countries passed laws regulating the flow of personal data. In 1980, the Organization for Economic Cooperation and Development (OECD) recommended a set of guidelines on data privacy and the transfer of information across borders. Although not legally enforceable, these guidelines emerged as a significant consensus on principles for protecting an individual’s privacy.

In the mid-1990s, the European Union enacted the EU Data Protection Directive 95/46/EC (the “Directive”) to unify data privacy regulations and promote the free flow of information among EU member states. Effective October 25, 1998, the Directive established minimum legal standards for data privacy protection and required member states either to enact new data privacy laws or amend existing laws to satisfy these minimum standards.

In some instances, countries outside Europe also have used the Directive as a model for their data privacy laws, or have proposed or are considering similar laws.

However, because the Directive contains only minimum standards, legislation varies from country to country within the EU, and sometimes includes stricter requirements. As such, companies that collect and process data within EU member states or transfer data from the EU need to understand and comply with each member state’s national law.

This Global Data Privacy Desk Reference summarizes the relevant laws in countries around the world. The following explanation of the basic principles of the Directive is intended to offer a more detailed introduction to European data privacy regulation.

Definitions

The EU Data Protection Directive includes the following definitions:

- **Personal data** is “any information relating to an identified or identifiable natural person.” Name, address, social security or other identification number, birthdate, telephone number or any other information that identifies an individual constitutes personal data.

- **Processing of personal data** is “any operation … which is performed upon personal data, whether or not by automatic means.” Examples include collecting, recording, storing, organizing, altering, retrieving, using, disclosing, transmitting, blocking, erasing or destroying data.

- **Data subject** is the person identified or identifiable by the personal data.

- **Data controller** is the person, agency or other entity that “determines the purposes and means of the processing of personal data.”

- **Consent** of the data subject is “any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.”

Collecting and processing personal data

The Directive requires that, before personal data may be processed, at least one of the following threshold conditions must be met:

- the data subject gives unambiguous consent;
- the data controller must process the data to perform a contract to which the data subject is a party (an employment contract, for example), or to take steps before entering a contract if the data subject requests it;
the data controller has a legal obligation and must process the data to comply with that obligation (tax withholding, for example);

• the processing is needed to protect the "vital interests" of the data subject;

• the processing is needed to perform a task carried out in the "public interest" or to exercise the data controller’s or a third party’s official authority; or

• the processing serves a legitimate interest of the data controller or a third party that is not overridden by the data subject’s fundamental rights and freedoms.

It can be difficult to determine whether processing personal data is in the “legitimate interest” of the data controller or whether the processing is needed to protect the data subject’s “vital interests.” Very little case law on these issues exists. As a result, obtaining the consent of the data subject is becoming the preferred method to legitimize data processing and transfer; multi-national companies have taken to incorporating specific consent language in stock option agreements, consumer contracts, and employment contracts.

To be valid, however, consent must be “freely” and “unambiguously” given. The issue of consent in an employer/employee relationship has been addressed by the “Article 29 Working Party,” an independent advisory board set up by the European Commission. The Working Party has questioned whether an employee is able to give a valid consent when the consent is a condition of employment. It advised that employers must give employees free choice on whether to give consent and permit them to withdraw consent anytime and without any adverse consequences such as the loss of employment or benefits. This conclusion is problematic for human resource activities since an employee’s name, social insurance ID and salary are typically needed to provide benefits, but it nonetheless stands as the Working Party’s current assessment.

If the processing of personal data is permissible under the Directive, data controllers are required to:

• collect the data for a specific purpose;

• hold the data only as long as needed;

• keep the data accurate plus up to date;

• inform the data subject why the data is being processed (companies often do this by including a disclosure as part of a consent form);

• identify the data controller and anyone receiving the data;

• keep the data secure; and

• give data subjects access to the data and a chance to correct any mistakes.

Except with the “explicit consent” of the data subject or the application of a few very limited exceptions, data collectors may not process sensitive data that reveals an individual’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sexual orientation.

Under national laws, many EU jurisdictions require data controllers to register their data processing activities and store databases with a local data protection authority. Companies are asked to make an initial filing at the start of the data processing that includes information about the data controller, the purpose for the database, and the types of data being collected. Data may only be processed for the stated purpose. Additional, annual filings also may be required.

Transferring personal data

Personal data may be transferred freely within the European Economic Area, which includes the 27 EU member states plus Iceland, Liechtenstein and Norway. Data controllers may also transfer data to countries recognized by the EU as providing “adequate protection” - protection equivalent to that mandated by the Directive - for the security of the data. These countries include Argentina, Canada, Switzerland, Guernsey and the Isle of Man. The EU is in the process of considering “adequacy finding” applications for Australia, New Zealand, Japan and South Korea.

The United States is not recognized by the EU as providing “adequate protection” because it lacks a comprehensive data protection law. Although the EU Data Protection Directive generally prohibits the transfer of personal data from EU member states to countries without “adequate protection,” there are a number of options that allow transfers to occur.

EU/US Safe Harbor

The US Department of Commerce and the EU negotiated a “Safe Harbor” agreement that permits the transfer of personal data out of EU member states.
to participating companies in the US. The agreement provides that any company subject to the jurisdiction of the US Federal Trade Commission or the Department of Transportation (excluding financial institutions and health providers) may revise its privacy policy to comply with seven safe harbor principles, publicly disclose the privacy policy, unambiguously and publicly disclose its dedication to the safe harbor principles, and certify compliance with the US Department of Commerce. EU companies are free to transfer personal data to US companies that have safe harbor agreements, and US multi-nationals with safe harbor agreements may transfer personal data within the organization from EU countries to the United States. To date, about 800 US companies have implemented safe harbor agreements.

The safe harbor principles require:
- **Notice**: organizations must tell individuals why their personal data is being collected and used, how to contact the data collector, who will receive the data, and how the data’s use and disclosure will be limited;
- **Choice**: individuals must be able to choose whether their data will be disclosed to third parties or used for additional purposes;
- **Onward transfer**: organizations must make sure that third parties receiving the personal data will comply with safe harbor principles;
- **Access**: individuals must have access to their personal data and be able to see, fix or delete it;
- **Security**: organizations must keep the data secure;
- **Data integrity**: organizations must take reasonable steps to make sure the personal data is reliable and relevant to its purpose; and
- **Enforcement**: organizations must make sure that there are methods in place to enforce compliance with the principles.

**Transfer agreements**

If the EU/US Safe Harbor is not a viable option, the use of transfer agreements that include mandatory clauses approved by the EU Commission will also permit the transfer of personal data from within EU member states to countries without “adequate protection.” Both the sender and receiver of the personal data must sign the transfer agreement. The clauses, referred to as “standard contractual clauses,” require the receiving company to be bound by both the Directive’s personal data protections and any additional protections required by the sender’s national law. The receiver also agrees to be subject to the jurisdiction of the sender’s domicile, and both parties agree to be jointly and severally liable for any damages suffered by a data subject from unlawful data processing.

Transfer agreements can be useful because they specifically require compliance with local data protection laws by third-party administrators or parent companies. That assurance may be necessary before local data protection authorities permit a data transfer. Transfer agreements can also provide an alternative to obtaining employee consent for data transfers, and can allocate liability for violations of data protection laws by third-party administrators.

Under some EU member states’ laws, a transfer agreement will allow a company to avoid having to get permission from local authorities before transferring data to countries without adequate protection. However, other EU member states require local permission for all data transfers to countries without “adequate protection;” any company planning a data transfer from a member state should consult that country’s laws.

**Binding Corporate Rules**

Binding Corporate Rules (BCRs) spell out a company or corporate group’s legally-binding code of conduct for processing personal data. Most often used by multi-nationals, BCRs are submitted to a lead local data protection authority in a European Economic Area country (usually the country where the company has its European headquarters), which in turn forwards the BCRs to multiple data protection authorities for approval. Once approved, the BCRs legally bind the company and its subsidiaries.

BCRs are relatively new, and may not be appropriate for every multi-national. However, they offer an opportunity to create a cost-effective, sustainable framework for compliance with global data protection requirements.

**BCRs should:**
- require compliance with the Directive’s personal data protections;
- describe safeguards that ensure data protection, including practical guidelines for achieving compliance;
• spell out how compliance will be verified, including audit procedures and measures to be taken in the event of a breach;

• describe how data will be processed, including identifying the kinds of data, the purpose for the processing and how much data will be transferred across borders; and

• set out systems for reporting BCR changes, within the corporate group and to the appropriate data protection authorities.

In order for BCRs to be approved by an EEA authority, they must be:
• legally binding within the corporate group, for all of the companies in the group (e.g., as a code of conduct) and for all employees (e.g., as provisions in employment contracts or disciplinary procedures);

• legally binding on subcontractors (e.g., as obligations in subcontracts); and

• legally binding externally for the benefit of data subjects (depending on the jurisdiction, this can be provided unilaterally through the parent company or by giving data subjects legally enforceable rights under intra-group contracts).

The Article 29 Working Party recently adopted a standard application form for approval of BCRs. The form is intended to make it easier for multi-nationals to submit BCRs to supervisory authorities and coordinate procedures.

Derogations

Article 26(1) of the Directive, “Derogations,” allows transfers of personal data from EU member states to countries without “adequate protection” for the security of the data if any of the following conditions are met:

• the data subject unambiguously consents;

• the transfer is needed to perform a contract between the data subject and the controller, or to take steps to enter a contract at the subject’s request;

• the transfer is needed to perform a contract for the benefit of the data subject between the controller and a third party;

• the transfer is needed or legally required by an important public interest, or to establish, exercise or defend a legal claim;

• the transfer protects the data subject’s “vital interests;” or

• the transfer is made from a register open either to the public or to persons with legitimate interests.

A 2005 Article 29 Working Party opinion notes that these derogations were designed to deal with “a limited number of situations in which an exemption from the adequacy requirement for third country transfers was considered to be appropriate,” and that they should be strictly applied.
ARGENTINA

LAW

Article 43 of the Constitution of Argentina establishes the fundamental right of habeas data for the protection of an individual’s personal data. It is enforceable through a constitutional complaint. The collection, processing and transfer of personal data is also regulated by Law 25:326, in force since 2000, and its Regulatory Decree No. 1.558.01.

REGISTRATION

Employers must register any database that includes employees' personal data with the Argentine data privacy authorities.

COLLECTION AND PROCESSING

Employers may compile and use an employee’s personal data when any of the following conditions are met:

- the employee consents;
- the data comes from a public source;
- the data is limited to name, national identity document, tax or social security information, occupation, date of birth and domicile;
- the data originates from an employment contract and is needed to enter into or perform the contract.

A financial institution may compile and use certain personal information it receives from its customers.

TRANSFER

Employers may transfer an employee’s personal data out of the country when any of the following conditions are met:

- the employee consents;
- the data comes from a public source;
- the data is limited to name, national identity document, tax or social security information, occupation, date of birth, and domicile; or
- the data originates from an employment contract and is needed to enter into or perform the contract.

Because the European Union has determined that Argentina provides "adequate protection" for personal data, transfers of data from EU member countries to Argentina are considered to be in compliance with the EU Data Protection Directive 95/46/EC.

A financial institution may transfer out of the country certain personal information it receives from its customers.
**Rights and Responsibilities**

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.

Employers must supply any information an employee requests about his personal data, and amend, update or suppress the data when appropriate.

Employers must treat employees’ personal data as privileged, and take all necessary steps to ensure it remains secure and confidential.

Employers and any third parties to whom they assign the data are jointly and severally liable for compliance with all laws and regulations.
AUSTRALIA

**Law**

There are no express privacy provisions in the Federal Constitution or the constitutions of Australia’s six states. The Privacy Act 1988 set standards for collecting and handling personal information about individuals. It was amended by the Privacy (Private Sector) Act 2000, which establishes National Privacy Principles (NPPs). NPPs are the minimum privacy standards for private-sector personal data processing. Enforcement is by the Office of the Federal Privacy Commissioner.

**Registration**

There is no requirement to register or notify the privacy authorities of a database containing information regarding employees.

**Collection and Processing**

Companies with annual turnovers of three million or less Australian dollars are generally not required to comply with the Privacy Act. However, businesses that are holding companies, subsidiaries of, or are otherwise related to businesses with annual turnovers in excess of three million Australian dollars, among other conditions, are subject to the Act’s rules on personal data collection.

The employee records exemption to the Privacy Act will permit an employer to collect, store or use personal information in an employee’s record if the information is directly related to the present or past employment relationship. No employee consent is required and the NPPs do not apply.

In general, employee consent is required if the employer is collecting sensitive information about, for example, race, ethnicity, political opinions, party affiliations or religion, unless the collection is mandated by law.

As an alternative to the NPPs, the Privacy Act allows private sector employers to create their own privacy codes, as long as the codes either match or exceed NPP standards. The Federal Privacy Commissioner first must approve the code, and it becomes binding when the employer agrees to be bound by it. The government has introduced an amendment to the Privacy Act which would allow these privacy codes to reach records now exempt from the Act.

Employers not bound by an approved privacy code must comply with NPPs.

Workplace Relations Act regulations require employers to keep employment records concerning overtime, termination, pay, leave and other related matters. The regulations do not prevent an employer from publishing or disclosing these records to a third party. The Workplace Relations Regulations apply only to employees covered by a federal award under the Workplace Relations Act, an Australian workplace agreement, or a certified agreement.

**Transfer**

Under the employee records exemption, a private employer may typically transfer personal data out of Australia without employee consent as long as the transfer is directly related to a past or present employment relationship. The employer is not subject to the Privacy Act or NPPs and is not required to make any assurances about the recipient’s privacy standards.

If the employee records exemption does not apply, an employer must, along with other conditions, inform employees why the personal data is being sent and who is receiving it.

Employers should use transfer agreements when the transfer is to a country without personal data protection equal to NPP standards.
| RIGHTS AND RESPONSIBILITIES | Employees have the right to access and correct personal data records compiled under the Workplace Relations Act. Employers bound by either NPPs or privately developed privacy codes are required to make certain that the personal data they collect, use or disclose is accurate, complete and up to date. |
AUSTRIA

LAW
A member of the European Union, Austria implemented the EU Data Protection Directive 95/46/EC by enacting the Austrian Data Protection Act 2000. The Act creates a Data Protection Commission (DPC) and a Data Protection Council with the power to investigate and assure compliance.

REGISTRATION
In general, before processing employee data, employers must file notice with the DPC for registration in the Data Processing Register. The DPC notice must state the categories of anyone in or out of the country who might receive the data, and the legal basis for its transfer.

COLLECTION AND PROCESSING
Employers may compile and use employees’ personal data when the data processing is a legitimate part of the employers’ business or when it fulfills the employers’ contractual and other obligations to its employees.

If the employer has a works council, Austrian labor law may require the council’s consent to process and transfer employees’ personal data.

TRANSFER
Employers may transfer employees’ personal data out of the country without authorization from the DPC if any of the following conditions are met:

• the data is indirectly personal to its recipient;
• regulations authorize the transfer;
• the employee consents;
• the transfer is needed to fulfill the employee’s interest in a contract;
• the data was collected legitimately and is needed to establish, exercise or defend legal claims before a foreign authority; or
• the transfer is to a country with “adequate protection” for personal data, such as an EU member state.

If none of these conditions apply, transfer of an employee’s personal data to a country that does not provide adequate data protection requires a permit from the DPC. Use of an intercompany agreement containing, for example, “standard contractual clauses” is recommended to expedite DPC permission.

RIGHTS AND RESPONSIBILITIES
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

• give employees access to the data and a chance to correct any mistakes.
## Belgium

### Law
A member of the European Union, Belgium implemented the EU Data Protection Directive 95/46/EC with the Law of 11 December 1998. The law was executed and some provisions were made more specific through the Royal Decree of 13 February 2001.

### Registration
There is no requirement to register or notify the privacy authorities of a database containing information regarding employees.

### Collection and Processing
Employers may compile and use personal information about an employee when any of the following conditions are met:

- the employee consents;
- the employer needs the data to carry out the employment contract;
- the employer needs the data to meet a legal obligation;
- the processing protects an employee’s vital interests;
- the employer needs the data to act in the public interest or to exercise official authority granted to the employer or a third party who is given access to the data; or
- the data is needed to fulfill a legitimate interest of the employer or of a third party with access to the data, as long as the employee’s fundamental interests, rights and freedoms are not superseded.

### Transfer
Employers may transfer employees’ personal data out of the country if any of these conditions is met:

- the employee consents;
- the transfer is needed to carry out the employment contract;
- the transfer is needed to perform or conclude a contract in the employee’s interest made between the employer and a third party;
- the transfer is required by an important public interest or by law;
- the transfer protects the employee’s vital interests; or
- the data comes from a public register.

Transfer of an employee’s personal data to non-EU/European Economic Area countries is allowed if the countries provide “adequate protection.” Use of the standard transfer contract approved by Belgium also will permit employers to send data out of the country without employee consent.

For transfer of data to the United States, compliance with the US/EU Safe Harbor principles satisfies the requirements of Belgium’s transfer law.
<table>
<thead>
<tr>
<th><strong>Rights and Responsibilities</strong></th>
<th>Employers must do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• collect the data for a specific purpose;</td>
</tr>
<tr>
<td></td>
<td>• hold the data only as long as needed;</td>
</tr>
<tr>
<td></td>
<td>• keep the data accurate and up to date;</td>
</tr>
<tr>
<td></td>
<td>• inform the employees why the data is being processed;</td>
</tr>
<tr>
<td></td>
<td>• inform the employees of any third parties that will be receiving the data;</td>
</tr>
<tr>
<td></td>
<td>• keep the data secure and confidential; and</td>
</tr>
<tr>
<td></td>
<td>• give employees access to the data and a chance to correct any mistakes</td>
</tr>
</tbody>
</table>
**BRAZIL**

<table>
<thead>
<tr>
<th>LAW</th>
<th>Privacy rights exist under Brazil’s Constitution, Consumer Code, Habeas Data Law and Banking Secrecy Law. No law specifically refers to collecting, processing or transferring personal information about individual employees.</th>
</tr>
</thead>
<tbody>
<tr>
<td>REGISTRATION</td>
<td>There is no requirement to register or notify the privacy authorities of a database containing information regarding employees.</td>
</tr>
<tr>
<td>COLLECTION AND PROCESSING</td>
<td>In general, employers do not need employees’ consent to collect and process personal data that relates to the employment relationship. Employee consent or a court order is required by the Banking Secrecy Law when an employer collects an employee's financial information.</td>
</tr>
<tr>
<td>TRANSFER</td>
<td>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.</td>
</tr>
<tr>
<td>RIGHTS AND RESPONSIBILITIES</td>
<td>No specific rights and responsibilities.</td>
</tr>
</tbody>
</table>
### LAW
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.

### Registration
There is no requirement to register or notify the privacy authorities of a database containing information regarding employees.

### Collection and Processing
Under PIEDA, employers may collect, process and use personal data without an employee's consent when any of the following conditions are met:

- the employee clearly will benefit and his or her consent cannot be obtained in a timely way;
- the information is needed for a breach of contract or legal investigation and employee consent might affect its accuracy;
- the data is available to the public;
- the data will be used to investigate a violation of law;
- a life, health or security emergency exists;
- the data is needed for a statistical or scholarly study; or
- the data collection is for journalistic, literary or artistic purposes.

In general, PIEDA requires an employer to:

- obtain an employee’s consent before or while it collects the data and for any new use of the data;
- identify the purpose for collecting and using the data;
- be honest about the purpose for collecting the data, and limit its collection to that purpose;
- use or disclose the data only for the purpose for which it was collected; and
- be accountable for its data privacy practices and policies.

PIEDA requires an employee’s consent when an employer processes sensitive data concerning, for example, race, ethnic origin, political opinions, party affiliation or religion.

Under the Quebec Privacy Act, employers collecting personal data are required to:

- have a serious and legitimate interest in the information;
- state the purpose for its collection;
• obtain express consent from the employee that specifically identifies how the data will be used; and

• collect data only required for the intended purpose.

Under the Income Tax Act of Canada, an employer must get an employee’s written authorization to use his or her Social Insurance Number.

**TRANSFER**

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.

Because the European Union has decided that PIEDA provides “adequate protection” for personal data, transfers of data from EU member countries into Canada are considered to be in compliance with the EU Data Protection Directive 95/46/EC.

**RIGHTS AND RESPONSIBILITIES**

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.
# Chile

## Law

The Constitution of Chile establishes an individual’s right to privacy. The Law for the Protection of Private Life regulates the collection, processing and transfer of personal data.

## Registration

There is no requirement to register or notify the privacy authorities of a database containing information regarding employees.

## Collection and Processing

An employee must consent to the processing of personal data by an employer except when the data comes from a public record or the law specifically allows it.

Personal data can only be used for the purposes for which it was collected.

## Transfer

Employers must tell employees when they transfer personal data out of the country to third parties. Employee consent is not required.

## Rights and Responsibilities

Employers must tell employees:

- who is processing their personal data;
- what data is being used; and
- why it is being used.

Employees have the right to access the personal data held by their employers and to request a copy every six months.
# China

<table>
<thead>
<tr>
<th><strong>Law</strong></th>
<th>Limited privacy rights are provided under China’s Constitution and civil laws. No general data protection laws exist.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Registration</strong></td>
<td>There is no requirement to register or notify the privacy authorities of a database containing information regarding employees.</td>
</tr>
<tr>
<td><strong>Collection and Processing</strong></td>
<td>No law expressly requires employee consent when employers process personal data. However, employers are advised to tell employees about the processing.</td>
</tr>
<tr>
<td><strong>Transfer</strong></td>
<td>No law expressly requires employee consent to the transfer of their personal data out of the country, but obtaining employee consent is advised.</td>
</tr>
<tr>
<td><strong>Rights and Responsibilities</strong></td>
<td>No specific rights and responsibilities.</td>
</tr>
</tbody>
</table>
**Czech Republic**

**Law**

The Data Protection Act regulates the collection, processing and transfer of personal data. However, because the Czech Republic joined the European Union in May 2004, the Act will need to be revised to put into force the EU Data Protection Directive 95/46/EC.

**Registration**

Although it is not certain if all employers are subject to the requirement, employers in general must register with the Czech Office on Protection of Personal Data (the “Authorities”) before collecting or processing employees’ personal data. No registration is necessary if the data is collected and processed as part of an employer’s duties under the Czech Labor Code; however, the extent of this exemption is not clear.

**Collection and Processing**

Employers may collect personal data only with employees’ written consent. The consent must state:

- how much and what kind of data will be collected;
- why and how long the data will be kept;
- what methods will be used to collect and maintain the data;
- who will have access to and continue to process the data; and
- if the employer intends to process the data again in the future.

Employers are required to have a purpose for collecting the personal data and must limit the collection to that purpose; decide how the data will be processed and maintained; and collect the data openly.

**Transfer**

Employers may send personal data to another country if that country provides “adequate protection” for the data.

If the data is sent to a country that does not provide “adequate protection,” the employer is required to get a permit from the Authorities, who have seven days to either grant or reject the permit.

The permit will be granted, in general, if any of the following conditions are met:

- the employee consents;
- the transfer is needed to protect the employee’s rights or enforce the employee’s claims;
- the data comes from registers that are either public or available to people with provable legal interests;
- the transfer results from an international treaty that binds the Czech Republic;
- the transfer is needed to perform or conclude the employment contract or a contract in the employee’s interest;
• the transfer is crucial to saving the employee’s life or providing for his medical care;
• the transfer is expressly demanded by special legislation; or
• the transfer is required by a contract that benefits the employee, as long as the third party receiving the data agrees to protect it.

**Rights and Responsibilities**

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.
### DENMARK

#### LAW
The Danish Constitution of 1953 includes data protection and privacy provisions. A member of the European Union, Denmark implemented the EU Data Protection Directive 95/46/EC with the Act on Processing of Personal Data (the Act). The Act is enforced by the independent Data Protection Agency (DPA).

#### REGISTRATION
Although employers generally are required to notify the DPA before processing personal data, they are exempt from this requirement when the data concerns employees and is not “sensitive” personal data. When notification is required, the DPA records the data processing actions in a public register.

#### COLLECTION AND PROCESSING
Employers may process personal data about individual employees when any of the following conditions are met:

- the employee gives consent;
- the employer needs the data to carry out a contract to which the employee is a party (an employment relationship is considered this type of contract), or to enter a contract with the employee, at the employee’s request; or
- the employer needs the data to satisfy an employee’s legal obligation.

Unless a specific exemption such as the employee’s express consent applies, employers may not process sensitive data concerning, for example, employees’ race, ethnic origins, political opinions, party affiliations or religion.

Employees may withdraw their consent at any time.

#### TRANSFER
Employers may transfer employees’ personal data out of the country if any of the following conditions are met:

- the employee expressly consents;
- the transfer is needed either to carry out a contract between the employer and the employee, or to enter the contract when the employee requests it;
- the transfer is needed to carry out a contract made in the employee’s interest between the employer and a third party;
- the transfer is required by an important public interest or to establish, exercise or defend a legal claim;
- the transfer protects the employee’s vital interests;
- the data comes from registers that are either public or available to those who can show a legitimate interest;
- the data is needed to prevent, investigate or prosecute a criminal offense; to execute a sentence; or to protect a defendant, witness or other person involved in a criminal
proceeding; or

• the transfer safeguards public or national security.

Employers may transfer employees’ personal data to countries that provide “adequate protection” for the data’s security.

The DPA may authorize an employer to transfer personal data to a country that does not provide “adequate protection” if the employer provides safeguards that protect employees’ rights. The employer may also have to comply with other conditions. To obtain DPA authorization, employers are advised to use “standard contractual clauses.”

<table>
<thead>
<tr>
<th>RIGHTS AND RESPONSIBILITIES</th>
<th>Employers must do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• collect the data for a specific purpose;</td>
</tr>
<tr>
<td></td>
<td>• hold the data only as long as needed;</td>
</tr>
<tr>
<td></td>
<td>• keep the data accurate and up to date;</td>
</tr>
<tr>
<td></td>
<td>• inform the employees why the data is being processed;</td>
</tr>
<tr>
<td></td>
<td>• inform the employees of any third parties that will be receiving the data;</td>
</tr>
<tr>
<td></td>
<td>• keep the data secure and confidential; and</td>
</tr>
<tr>
<td></td>
<td>• give employees access to the data and a chance to correct any mistakes.</td>
</tr>
<tr>
<td><strong>EGYPT</strong></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td></td>
</tr>
<tr>
<td><strong>LAW</strong></td>
<td>The Egyptian Constitution establishes a basic right to a private life in limited provisions. There are no data protection laws.</td>
</tr>
<tr>
<td><strong>REGISTRATION</strong></td>
<td>There is no requirement to register or notify the privacy authorities of a database containing information regarding employees.</td>
</tr>
<tr>
<td><strong>COLLECTION AND PROCESSING</strong></td>
<td>No law expressly requires employee consent when employers process personal data. However, employers are advised to tell employees about the processing.</td>
</tr>
<tr>
<td><strong>TRANSFER</strong></td>
<td>No law expressly requires employee consent to the transfer of personal data out of the country, but obtaining employee consent before transfer is advised.</td>
</tr>
<tr>
<td><strong>RIGHTS AND RESPONSIBILITIES</strong></td>
<td>No specific rights and responsibilities.</td>
</tr>
</tbody>
</table>
The Constitution of Finland establishes traditional privacy rights. A member of the European Union, Finland implemented the EU Data Protection Directive 95/46/EC with the Personal Data Act which passed in 1999 and was amended in 2004, which applies to public and private sectors, and covers manual and automated files. The Act on the Amendment of the Personal Data Act adds provisions for transferring personal data out of the country. The Working Life Act concerns employer/employee relations and specifically governs the processing of employees’ personal data.

The Office of the Data Protection Ombudsman (DPO), an independent agency, directs, guides, supervises and consults on personal data processing. The Data Protection Board (DPB) deals with the application of the Personal Data Act. Both the DPO and DPB have authority to make decisions under the Personal Data Act.

Employers generally must disclose data processing activities to the DPO. However, disclosure is not necessary when:

- the employee clearly consents;
- the employer needs the data either to carry out a contract to which the employee is a party or to enter a contract with the employee, at the employee’s request; or the processing protects an employee’s vital interests.

Under the Working Life Act, employers may process personal data only if the processing is required to manage the rights and obligations involved in the employer/employee relationship or to manage the employee’s benefits, or if the processing is connected to the special nature of the employee’s work. There are no exceptions, even with employee consent.

The Working Life Act generally requires employers to collect personal data from employees. Data may be collected from third parties, but only with employee consent. Consent will not be required, however, if other exemptions apply; for example, if the employer needs access to an employee’s credit status or criminal history.

Unless an exemption such as the employee’s express consent applies, employers may not process sensitive data concerning, for example, employees’ race, ethnic origins, political opinions, party affiliations or religion.

Employers are also generally required to comply with the Personal Data Act. Under its guidelines, an employer may process personal data when any of the following conditions are met:

- the employee clearly consents;
- the employer needs the data either to carry out a contract to which the employee is a party (the employment relationship is considered a type of contract); or to enter a contract with the employee, at the employee’s request;
- the processing protects an employee’s vital interests;
- the processing meets a legal obligation;
- a relevant connection exists between the employer’s operations and the employee’s service.
to the employer; or

• the data relates to employees of a group of companies or other similar economic group, and is processed within that group.

**TRANSFER**

Employers may transfer employees’ personal data out of the country without notifying the DPO when any of the following conditions are met:

• the employee clearly consents;

• the transfer is needed to carry out a contract to which the employee is a party;

• the transfer is to a country that ensures “adequate protection” for personal data (this includes EU member states and European Economic Area countries); or

• the transfer agreement contains “standard contractual clauses.”

For data transfers to the United States, compliance with the US/EU Safe Harbor principles equals compliance with the international data transfer laws of Finland.

**RIGHTS AND RESPONSIBILITIES**

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.
# France

## Law

The Data Processing, Data Files and Individual Liberties Law of 1978 (the Law) regulates the collection, processing and transfer of personal data. It was amended, effective August 2004, to bring France, a member of the European Union, into compliance with the EU Data Protection Directive 95/46/EC. The Law is enforced by the Commission Nationale de l'Informatique et des Libertes (CNIL).

## Registration

Employers must provide the CNIL with mandatory information and a commitment that their planned processing of personal data complies with the Law.

If data will be transferred out of the country, the notice must specify what kind of data it is, why and how it will be collected and what country will receive it. An agreement between the employer and the recipient containing the recipient’s agreement to comply with French data privacy laws must be included in the notification.

No processing may occur until the CNIL acknowledges that it has received the notification. Some notice requirements are waived, however, if an employer has appointed a data protection officer.

Before introducing or changing an automated system for data processing, employers must notify and consult with the Works Council.

## Collection and Processing

Employers may process personal data only if the data is directly connected to a job or to an employee’s ability to do the job.

Before collecting personal data, employers must:

- ask employees if they want to provide the data;
- tell employees how they will collect the data, why it is being collected, and who will see it;
- give employees the option to refuse to provide the data and tell them what will happen if they do refuse; and
- tell employees they have the right to see and fix the data or withdraw their consent.

Without employee consent, employers may collect and process personal data when it is essential to the company’s legitimate interests, unless the employee’s fundamental rights, interests or freedoms take precedence.

Employee consent is required when sensitive data concerning, for example, race, ethnic origin, political opinions, party affiliations or religion will be processed. However, in an employment context, employee consent may still be subject to challenge on the basis that it was not freely given.

## Transfer

Employers may transfer personal data out of the country when any of the following conditions are met:

- the employee consents (however, such consent may still be subject to challenge on the basis
that it was not freely given);

• the transfer is needed to carry out the employment contract;
• the transfer is needed to carry out a contract in the employee’s interest made between the employer and a third party;
• the transfer is required by an important public interest or by law;
• the transfer protects the employee’s vital interests; or
• the data comes from a public source.

An employer may never transfer an employee’s social insurance number out of the country for identification purposes.

The transfer of personal data to non-EU/European Economic Area countries is permitted if the receiving countries provide “adequate protection.”

The transfer of personal data in accordance with “standard contractual clauses” will enable transfer, according to an EU Commission ruling, although France hasn’t expressly approved a standard contract.

France will accept transfer agreements with non-standard contract clauses or codes of conduct, but only if they include sufficient safeguards to protect an employee’s privacy rights and the exercise of those rights. CNIL authorization is also required. The CNIL is in favor of the use of binding corporate rules.

For transfer of data to the United States, compliance with the US/EU Safe Harbor principles satisfies the requirements of France’s transfer law.

### Rights and Responsibilities

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.
GERMANY

LAW
A member of the European Union, Germany implemented the EU Data Protection Directive 95/46/EC in May 2001 by amending the German Federal Data Protection Act.

REGISTRATION
To transfer sensitive personal data inside or out of the country, an employer must register with the local data protection authority by submitting a form. The form generally requires the following information:

• the company’s name and address;
• who manages the company;
• who will process the data;
• the name, address and other relevant information about the data protection officer, if there is one;
• why the data is being processed and used;
• who will be affected;
• if the data will be transferred inside Germany or to an EU country, who will receive it;
• if the data will be transferred out of the country to non-EU countries, who will receive it, what kinds of data are included, and how the data will be kept secure.

There is no fee and no approval is required.

COLLECTION AND PROCESSING
Employers may collect and process personal employee data when any of the following conditions are met:

• the employee consents;
• the processing serves the employment agreement’s purpose;
• the processing protects the employer’s valid interests and the employee has no prevailing, legitimate interest in preventing it;
• the data is either publicly available or the employer has the right to publish it, unless the employee has a prevailing reason to prevent its use;
• the processing is needed to protect the public interest or a third party’s legitimate interest, and the employee has no legitimate interest in preventing it; or
• the processing is allowed by a national law such as a collective labor agreement.

An employee must explicitly consent if the employer is processing sensitive data concerning, for example, race, ethnic origin, political opinions, party affiliation or religion. No consent is required, however, if the data is needed to proceed with or defend against a legal claim, or if it concerns an
employee’s health and relates to his sick leave.

If an employer has more than four employees involved in the “automated processing of data,” (including computer processing), the employer must appoint a data protection officer. The officer may be an employee but may not be part of management, and must attend some of the seminars on data protection offered throughout the country. To make sure that the employer complies with data privacy laws, the officer must hold an independent position.

**TRANSFER**

Employers may transfer personal data out of the country if any of the following conditions is met:

- the employee consents;
- the transfer is needed to carry out the employment contract;
- the transfer is needed to carry out a contract in the employee’s interest made between the employer and a third party;
- the transfer is required by an important public interest or by law;
- the transfer protects the employee’s vital interests; or
- the data comes from a public register.

Employers may not transfer employees' personal data to a trade union so the union can collect a debt, or to an insurance company for use in advertising.

The transfer of personal data to European Economic Area countries will be restricted if the data processing falls outside the scope of what is allowable under the EU Data Protection Directive 95/46/EC.

The transfer of personal data to non-EU/European Economic Area (EEA) countries is permitted if the receiving countries provide “adequate protection” for the security of the data.

Germany has approved a standard contract for out-of-country transfers that does not require employee consent. Non-standard contracts or codes of conduct will also work if they have sufficient protection for employees' privacy rights and the exercise of those rights, and if the transfer has been approved by an acceptable supervising authority.

For transfer of data to the United States, compliance with the US/EU Safe Harbor principles satisfies the requirements of Germany’s transfer law.

**RIGHTS AND RESPONSIBILITIES**

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
**Greece**

**Law**
The Constitution of Greece establishes traditional privacy rights, and a 2001 Constitutional amendment creates an express right for individuals to protect their personal data. A member of the European Union, Greece implemented the EU Data Protection Directive 95/46/EC in 1997 with the Law on the Protection of Individuals with regard to the Processing of Personal Data. An independent agency, the Hellenic Data Protection Authority (DPA), regulates and oversees the collection and processing of personal data.

**Registration**
In general, employers must inform the DPA when they process personal data so the processing can be registered in the Files and Data Processing Register. No notification or registration is required, however, when the employer gives employees advance notice, the processing relates directly and only to their employment relationship, and the processing either satisfies a legal obligation or meets an employment-related obligation.

**Collection and Processing**
Employers may process employees’ personal data when any of the following conditions are met:

- the employee consents;
- the employer needs the data either to carry out a contract to which the employee is a party (the employment relationship is considered this type of contract), or to take action before entering a contract if the employee requests it; or
- the employer needs the data to satisfy a legal obligation.

Employers planning to process sensitive data concerning, for example, race, ethnic origins, political opinions, party affiliations or religion, generally need to get a permit from the DPA. No permit will be necessary, however, when the employer gives employees advance notice, the processing relates directly and only to their employment relationship, and the processing either satisfies a legal obligation or meets an employment-related obligation.

**Transfer**
Employers may transfer employees’ personal data to other EU-member states.

Employers planning to send personal data (processed or intended for processing) to a non-EU country must first get a DPA permit. The permit will be issued if the country ensures “adequate protection” for the security of the data.

For countries that do not ensure “adequate protection,” a permit may be granted and the transfer allowed if any of the following conditions are met:

- the employee consents;
- the transfer is needed to carry out a contract between the employer and employee;
- the transfer is needed to carry out a contract between the employer and a third party when it serves the employee’s interests; or the transfer must take place before a contract can be entered and the employee requests it.
### Rights and Responsibilities

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.
## Law
The Hong Kong Personal Data Privacy Ordinance (PDPO) regulates the collection, transfer and processing of personal data. The PDPO incorporates the principle requirements of the Organization for Economic Cooperation and Development Guidelines and the EU Data Protection Directive 95/46/EC. The Office of the Privacy Commissioner is charged with enforcing the PDPO and has clarified its provisions by issuing nonbinding Codes of Practice.

## Registration
Employers may be required to submit a data user return form containing specified data to the Privacy Commissioner. There is a set fee.

## Collection and Processing
An employer may compile and use personal information about employees only for the purpose it has outlined in a Personal Information Collection (PIC) Statement. Consent of the employee is required if the data is to be used for any other purpose.

## Transfer
Employers are permitted to transfer employees’ personal data out of the country if any of the following conditions are met:

- the employee consents;
- the employer reasonably believes that the government in the receiving country has enacted a law similar to the PDPO;
- the employer has taken "all reasonable precautions and exercised all due diligence" to insure the foreign processing of the data will not breach any provisions of the PDPO;
- the employee’s contractual rights and benefits are not adversely affected, or the adverse effect is mitigated;
- the transfer is necessary to safeguard Hong Kong’s security, defense or international relationships;
- the transfer is necessary to establish, exercise or defend legal claims, as long as any adverse action against the employee is avoided or mitigated; or
- the transfer is necessary to protect the employee’s vital interests.

Employers may be permitted to transfer an employee’s personal data out of the country when the transfer is needed to perform or conclude a contract between the employer and a third party, if the contract is in the employee’s interest.

For transfer of data to the United States, compliance with the US/EU Safe Harbor principles satisfies the requirements of the PDPO.

Although Hong Kong does not have a statutory standard form of contract, the Privacy Commissioner has issued a model contract for the transfer of personal data from an employer to a third party. The Privacy Commissioner apparently has taken the position that a code of conduct alone is not sufficient.
The PDPO gives the Privacy Commissioner the power to publish a list of countries permitted to receive personal data, but no list has been published.

<table>
<thead>
<tr>
<th>RIGHTS AND RESPONSIBILITIES</th>
<th>Employers processing personal data must provide notice to employees in a PIC statement that includes:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• why the data is being collected;</td>
</tr>
<tr>
<td></td>
<td>• what happens to the employee if he or she does not provide the requested data;</td>
</tr>
<tr>
<td></td>
<td>• the employee’s right to see the data and ask for corrections if necessary;</td>
</tr>
<tr>
<td></td>
<td>• who is responsible for the employer’s data protection policies and how the employee can contact that person;</td>
</tr>
<tr>
<td></td>
<td>• what the procedures are for seeing and correcting the data held by the employer; and</td>
</tr>
<tr>
<td></td>
<td>• whether the data will be transferred, and the names or categories of everyone likely to receive it.</td>
</tr>
</tbody>
</table>

PIC statements should be given to applicants for job postings, through a link if data is collected in a website, and to employees when they start work.
### Hungary

<table>
<thead>
<tr>
<th>Law</th>
<th>The Constitution of Hungary establishes traditional privacy rights and protects an individual's personal data. Private and public sector use and collection of personal data is controlled by Act No. LXIII of 1992 on the Protection of Personal Data and the Publicity of Data of Public Interest. Because Hungary joined the European Union in May 2004, the Act will need to be revised to implement the EU Data Protection Directive 95/46/EC.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration</td>
<td>Although there is a general requirement for reporting data processing activities to the Commissioner for registration in the Data Processing Register, the requirement typically will not apply to the processing of employee data by employers.</td>
</tr>
<tr>
<td>Collection and Processing</td>
<td>Employers must obtain employee consent before processing personal data, unless the processing is required by law. Processing can only be done for a specific purpose. Employers may not process sensitive data concerning, for example, race, ethnic origin, political opinions, party affiliations or religion, unless the employee gives written consent or the processing is required by law.</td>
</tr>
<tr>
<td>Transfer</td>
<td>Employers may not send personal data to countries without “adequate protection” for the data’s security, unless the employee consents or the law allows it. The law is not clear on the use of an intercompany agreement.</td>
</tr>
<tr>
<td>Rights and Responsibilities</td>
<td>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.</td>
</tr>
</tbody>
</table>
## India

### Law
There is no express right to privacy in India’s 1950 Constitution, but the Supreme Court has recognized an implicit right to privacy under Article 21 of the Constitution. Only general principles of Indian law apply to the protection and confidentiality of data supplied by an employee to an employer. However, the Information Technology Act 2000 and other acts provide some sectoral protection. In July 2004, the government declared its intent to amend a number of statutes, including the Information Technology Act 2000; the Indian Penal Code; the Indian Contracts Act, 1872; the Consumer Protection Act, 1986; and the Specific Relief Act, 1963 to include sections on data privacy and security.

### Registration
There is no requirement to register or notify the privacy authorities of a database containing information regarding employees.

### Collection and Processing
There is no express requirement for employers to obtain employees’ consent for processing personal data. However, because India is expected to enact data protection laws, employers are advised to tell employees about data processing activity.

### Transfer
There is no express requirement for employers to obtain employee consent before their personal data is sent out of the country. However, because India is expected to enact data protection laws, employers are advised to have a legal reason for the transfer (an employment relationship suffices) and to get the employee’s consent.

### Rights and Responsibilities
No specific rights and responsibilities.
<table>
<thead>
<tr>
<th><strong>INDONESIA</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LAW</strong></td>
</tr>
<tr>
<td>The Indonesian Law on Human Rights establishes the basic right to a private life. A Bill on Electronic Information and Transaction was submitted to the Indonesian president in July 2005 but is still pending.</td>
</tr>
<tr>
<td><strong>REGISTRATION</strong></td>
</tr>
<tr>
<td>There is no requirement to register or notify the privacy authorities of a database containing information regarding employees.</td>
</tr>
<tr>
<td><strong>COLLECTION AND PROCESSING</strong></td>
</tr>
<tr>
<td>No law expressly requires employee consent when employers process personal data. However, employers are advised to tell employees about the processing.</td>
</tr>
<tr>
<td><strong>TRANSFER</strong></td>
</tr>
<tr>
<td>No law expressly requires employee consent to the transfer of personal data out of the country, but obtaining employee consent is advised.</td>
</tr>
<tr>
<td><strong>RIGHTS AND RESPONSIBILITIES</strong></td>
</tr>
<tr>
<td>No specific rights and responsibilities.</td>
</tr>
</tbody>
</table>
## Ireland

### Law

### Registration
Before processing personal data, some types of employers (financial institutions, insurance companies and companies that hold sensitive data among them) must register with the DPC.

### Collection and Processing
Employers may process employees’ personal data when any of the following conditions are met:

- the employee consents;
- the employer needs to process the data to carry out a contract to which the employee is a party (the employment relationship is considered in this type of contract), or to take action before entering a contract if the employee requests it;
- the processing satisfies the employer’s legal obligation;
- the processing protects the employee’s vital interests;
- the processing is needed for a public purpose; or
- the employer has a legitimate reason for the processing (for personnel or human resource purposes, for example), and it doesn’t unreasonably harm the employee’s fundamental rights, freedoms or legitimate interests.

Employers may process sensitive data concerning, for example, race, ethnic origin, political opinions, party affiliations or religion, but only when one of the above conditions applies and, in addition, one of the following requirements is met:

- the employee’s consent is explicit;
- the processing is required to satisfy a right created or obligation imposed by employment law; or
- the processing is needed for a public purpose.

### Transfer
Transfer of personal data out of the country but within a multinational group for normal personnel and human resources uses does not require explicit employee consent. The consent is considered to be implied when the employer is a multinational company.

Employers may send personal data to a country outside the European Economic Area if the EU Commission or the DPC determines that the country ensures “adequate protection” for the data’s security.

Employers may send personal data to countries outside the EEA who do not have “adequate protection” if:

- the employee consents;
- the processing is required to satisfy a right created or obligation imposed by employment law; or
- the processing is needed for a public purpose.
protection” for data if any of the following conditions are met:

- the employee consents;
- the transfer is required or permitted by a law, convention or instrument that places a duty on the State;
- the transfer is needed to carry out a contract between the employer and employee;
- the transfer must take place before a contract between the employer and employee can be entered;
- the transfer is needed to carry out a contract between the employer and a third party when the contract serves the employee’s interests and the employee requests it;
- the employer needs to make the transfer to get legal advice;
- the transfer will protect the employee’s health or prevent his injury and is urgent;
- the data is available on a public register;
- the DPC authorizes the transfer after seeing evidence from the employer that employees’ fundamental rights and freedoms will be adequately safeguarded; or
- the terms of the transfer are the kinds of terms the DPC has approved as providing adequate safeguards of employees’ fundamental rights and freedoms; examples include “standard contractual clauses” and US/EU Safe Harbor principles.

**Rights and Responsibilities**

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.
ISRAEL

<table>
<thead>
<tr>
<th>LAW</th>
<th>Section 7 of the Basic Law on Human Dignity and Freedom (1992) establishes a right to privacy in Israel. The Protection of Privacy Law 1981 controls data privacy protection; it is enforced by the Registrar of Databases.</th>
</tr>
</thead>
<tbody>
<tr>
<td>REGISTRATION</td>
<td>Employers are required to register databases that include either more than 10,000 names or some kinds of confidential information. Registration is with the Registrar of Databases and must specify why and how the data is being collected, how the database will be used, and how the data will be kept secure.</td>
</tr>
<tr>
<td>COLLECTION AND PROCESSING</td>
<td>Employers are not required to obtain employee consent for processing personal data except when the data is collected for one purpose and then used for another.</td>
</tr>
<tr>
<td>TRANSFER</td>
<td>Employers may transfer employees’ personal data out of the country without their consent only when the receiving country has “adequate safeguards” for the data’s security or the transfer is covered by an intercompany transfer agreement. For transfers to Israel from European Union countries, the European Commission has found that Israel’s data privacy laws probably offer “adequate protection.”</td>
</tr>
<tr>
<td>RIGHTS AND RESPONSIBILITIES</td>
<td>Employers must give employees access to their personal data.</td>
</tr>
</tbody>
</table>
ITALY

LAW

The Constitution of Italy establishes a traditional right to privacy. A member of the European Union, Italy implemented the EU Data Protection Directive 95/46/EC with Law No. 675 of December 1996. The law controls public and private sector personal data processing; it is enforced by the Supervisory Authority for Personal Data Protection (the Authority).

REGISTRATION

Before processing employees’ personal data, employers are required to register with the Authority, unless the processing is done solely to meet personnel and human resource obligations and the data is kept only as long as it is needed.

COLLECTION AND PROCESSING

Employers may process personal data when any of the following conditions is met: • the employee consents;

- the employer needs to process the data to carry out a contract to which the employee is a party (the employment relationship is considered this type of contract), or to take action before entering a contract if the employee requests it; or

- the processing satisfies a legal obligation.

Both written consent from the employee and authorization from the Authority are required when the employer processes sensitive data concerning, for example, race, ethnic origin, political opinions, party affiliations or religion.

TRANSFER

Employers may transfer personal data to countries outside the European Union when any of the following conditions are met:

- the employee consents;

- the transfer is needed to carry out a contract to which the employee is a party;

- the transfer must take place before a contract can be entered, when the employee requests it;

- the transfer is needed to carry out a contract made in the employee’s interest; or

- the Authority authorizes the transfer.

The Authority has authorized transfers to non-EU countries when the transfers are covered by "standard contractual clauses" or where the receiving country’s laws ensure “adequate protection” for the data’s security.

For data transfer to the United States, compliance with US/EU Safe Harbor principles satisfies the requirements of Italy’s transfer law.

RIGHTS AND RESPONSIBILITIES

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
**Japan**

**Law**
The Personal Information Protection Law, passed in May 2003, governs collecting, processing and transferring personal data by companies in Japan that store information on more than 5,000 individuals. Earlier codes of practice provided nominal regulation of private sector data collection in some sectors.

**Registration**
There is no requirement to register or notify the privacy authorities of a database containing information regarding employees.

**Collection and Processing**
When collecting or processing personal data, employers must tell employees directly how they intend to use the data. The collection must be limited to what is necessary to achieve that goal. Because consent is implied in Japan, employees must “opt out,” or withdraw their consent, if they object.

- When it is difficult to give employees the opportunity to opt out, employers may collect and process personal data when any of the following conditions applies:
  - the use or disclosure of the data is required by a law, ordinance or official order;
  - the processing is needed to protect life, safety or property; or
  - the processing is needed to promote public health.

Employers may use a database containing employees’ personal information only for its original intended use. Any new use requires a new notification to employees, who may withdraw consent or prevent the transfer of their personal data to a third party.

**Transfer**
Employers may not transfer data to third parties without first obtaining consent from employees except if one of the following conditions applies:

- the employer delegates some or all of the data processing activities to another company located in or outside of Japan;
- the employer gives the data to a successor company in a merger; or
- the employer is sharing the data with companies in the same field who plan to use it for its intended purpose, but only if the employee is told or can easily find out about the transfer.

**Rights and Responsibilities**
Employers must describe how personal data will be used directly to employees. If the data processing relates to performance of the employment contract, notice of its intended use must be made before collection begins. Any new use requires a new notification.

Employers may avoid the disclosure requirement when they legitimately believe that disclosure will harm their rights or fair profits.

Employers must keep personal data current and correct, and take steps to prevent the data from
being improperly disclosed, lost or destroyed.

Employees may "opt out" and withdraw their consent to the collection and processing of their personal data, with some exceptions.

Employees may ask that their personal data be updated or corrected.

If employers change the intended use of the data, employees may withdraw consent for its use or transfer to a third party. Employers may refuse the request if the cost is too high, as long as they find another way to safeguard the employees' welfare.
**LITHUANIA**

**LAW**

The Constitution of Lithuania establishes traditional privacy rights. The Law on Legal Protection of Personal Data regulates the collection, processing and transfer of personal information about individuals. It was amended after Lithuania joined the European Union in May 2004, to bring the law into compliance with the EU Data Protection Directive 65/46/EC. The law is enforced by the State Data Protection Inspectorate (SDPI).

**REGISTRATION**

Employers planning to process sensitive data concerning, for example, race, ethnic origin, political opinions, party affiliations or religion, first are required to register with and be authorized by the SDPI.

**COLLECTION AND PROCESSING**

Employers may collect and process personal data when any of the following conditions are met:

- the employee consents;
- the employer needs the data to carry out the employment contract;
- the employer needs the data to comply with a legal obligation;
- the processing protects the employee’s vital interests;
- the processing is necessary to act in the public interest or to the exercise of official authority by the government or an authorized third party in receipt of the data; or
- the data is needed to fulfill a legitimate interest of the employer or a third party in receipt of the data, but only if the employees’ fundamental rights remain protected.

**TRANSFER**

In general, SDPI authorization is required before an employer may transfer employees’ personal data out of the country.

The SDPI will authorize transfers to countries with “adequate protection” for the security of the data, and to countries with inadequate protection if the transfer is covered by a contract that includes adequate safeguards.

The SDPI will also authorize transfers out of the country if any of the following conditions are met:

- the employee consents;
- the transfer is needed to carry out a contract between the employer and the employee;
- the transfer must take place before a contract can be concluded, when the employee requests it; or
- the transfer is needed to carry out a contract made in the employee’s interest between the employer and a third party.
<table>
<thead>
<tr>
<th>RIGHTS AND RESPONSIBILITIES</th>
<th>Employers must do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• collect the data for a specific purpose;</td>
</tr>
<tr>
<td></td>
<td>• hold the data only as long as needed;</td>
</tr>
<tr>
<td></td>
<td>• keep the data accurate and up to date;</td>
</tr>
<tr>
<td></td>
<td>• inform the employees why the data is being processed;</td>
</tr>
<tr>
<td></td>
<td>• inform the employees of any third parties that will be receiving the data;</td>
</tr>
<tr>
<td></td>
<td>• keep the data secure and confidential; and</td>
</tr>
<tr>
<td></td>
<td>• give employees access to the data and a chance to correct any mistakes.</td>
</tr>
</tbody>
</table>
## MEXICO

### LAW
The Constitution of Mexico establishes traditional privacy rights. There are no explicit data protection laws; however, parts of the Federal Labor Law and the Federal Criminal Code can be read to protect employees’ privacy and restrict the transfer of personal data. A proposed law similar to the European Union Data Protection Directive 95/46/EC has been bottled up in the Mexican Congress since 2002.

### REGISTRATION
There is no requirement to register or notify the privacy authorities of a database containing information regarding employees.

### COLLECTION AND PROCESSING
Because a data protection law could be enacted soon, employers are advised to disclose data processing activities to employees. However, employee consent is not specifically required.

### TRANSFER
At this time, no law specifically requires employee consent to the transfer of personal data out of the country, but employers are advised to obtain consent.

### RIGHTS AND RESPONSIBILITIES
No specific rights and responsibilities.
THE NETHERLANDS

LAW
The Constitution of the Netherlands establishes traditional privacy rights and protects an individual’s personal data. A member of the European Union, the Netherlands implemented the EU Data Protection Directive 95/46/EC by amending and expanding the Data Registration Act of 1998 with the Personal Data Protection Act 2000 (the Act). The Act is enforced by the Dutch Data Protection Authority (DPA).

REGISTRATION
Some categories of manual and automated databases must be supplied to the DPC for inclusion in a public register; however, personnel and human resources data does not need to be reported or registered.

COLLECTION AND PROCESSING
Employers may collect and process employees’ personal data for stated, clearly-defined and legitimate purposes related to the employment relationship. Employers are limited to using data that specifically relates to, satisfies and does not exceed those purposes.

Employers may process employees’ personal data when any of the following conditions are met:

• the employee clearly and explicitly consents;
• the employer needs to process the data to carry out a contract to which the employee is a party (the employment relationship is considered this type of contract), or to take action before entering a contract, if the employee requests it;
• the processing satisfies the employer’s legal obligation;
• the processing protects the employee’s vital interests;
• the processing allows performance of a legal duty; or
• the employer, or a third party in receipt of the data, has a legitimate reason for the processing and it doesn’t unreasonably harm the employee’s rights and freedoms, especially the employee’s right to privacy.

Except when an employer must process data about an employee’s race for purposes of identification or affirmative action, employers may not process sensitive data concerning, for example, race, ethnic origin, political opinions, party affiliations or religion, without the employee’s explicit consent.

The DPC will review a code of conduct submitted by an employer to determine if the code complies with data processing laws and regulations.

TRANSFER
Employers in compliance with the Act may transfer personal data out of the Netherlands to EU member states or non-EU countries with “adequate protection” for the data’s security.

Employers may transfer personal data to countries with inadequate data protection when any of the following conditions are met:

• the employee clearly and explicitly consents;
• the transfer is needed to carry out a contract between the employer and the employee;
• the transfer must take place before a contract is completed, if the employee requests it;
• the transfer is needed to carry out a contract made in the interest of the employee between the employer and a third party; or
• the employer has applied for and received a permit from the Minister of Justice allowing the transfer (use of "standard contractual clauses" is helpful).

### RIGHTS AND RESPONSIBILITIES

<table>
<thead>
<tr>
<th>Rights and Responsibilities</th>
<th>Employers must do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• collect the data for a specific purpose;</td>
</tr>
<tr>
<td></td>
<td>• hold the data only as long as needed;</td>
</tr>
<tr>
<td></td>
<td>• keep the data accurate and up to date;</td>
</tr>
<tr>
<td></td>
<td>• inform the employees why the data is being processed;</td>
</tr>
<tr>
<td></td>
<td>• inform the employees of any third parties that will be receiving the data;</td>
</tr>
<tr>
<td></td>
<td>• keep the data secure and confidential; and</td>
</tr>
<tr>
<td></td>
<td>• give employees access to the data and a chance to correct any mistakes.</td>
</tr>
</tbody>
</table>
## NEW ZEALAND

### LAW

Courts have held that Article 21 of the New Zealand Bill of Rights establishes privacy rights. The Privacy Act of 1993 creates 12 Information Privacy Principles (IPPs) that regulate the private and public collection, use and transfer of personal data. The Act is enforced by the Office of the Privacy Commissioner.

### REGISTRATION

There is no requirement to register or notify the privacy authorities of a database containing information regarding employees.

### COLLECTION AND PROCESSING

Employers may collect personal data from employees as long as the employer needs the data in the lawful course of business.

Employers are required to get the personal information directly from employees unless it is not reasonably practical to do so or the information is publicly available.

An employer must appoint a Privacy Officer to oversee compliance with the Act. A staff member can do the job in addition to his or her regular assignment.

Employers may be subject to codes of practice issued by the Privacy Commissioner for specific industries, agencies or kinds of data. The codes may make the IPPs more or less strict.

### TRANSFER

Employers may send personal data out of the country with employee consent or when the transfer directly serves the purpose for which the data was collected.

Employers may also send data out of the country if the recipient abides by some number of IPPs.

### RIGHTS AND RESPONSIBILITIES

Employers must give employees the following information either before collecting their personal data or as soon as possible after collecting it:

- how the data is being collected;
- why it is being collected; and
- who will receive and keep the data.

Notice is not required if employees consent to the non-disclosure or non-disclosure will not harm employees’ interests.

Employers must make sure that employees’ personal data is not lost, changed, disclosed or misused, and should keep the data only as long as is needed to satisfy its lawful purpose.

Employees have the right to see and correct their personal data.
Norway

Law

There is no specific right to privacy in the Norwegian Constitution of 1814. The Personal Data Act of 2000, which governs public- and private-sector personal data processing, implements the EU Data Protection Directive 95/46/EC, even though Norway is a member of the European Economic Area but not the European Union. The Act is enforced by the Data Inspectorate.

Registration

Before processing sensitive data that has not been provided voluntarily by an employee, an employer must get a license from the Inspectorate.

A license will not be required, however, if the employee consents, the data concerns the employment relationship, and the data will be used for human resources/employee administration purposes.

The Inspectorate may also require an employer to get a license if it determines that the personal data processing will violate employees’ substantial privacy interests.

Employers have the right to demand a ruling on whether processing is subject to a licensing requirement.

Collection and Processing

Employers may process employees’ personal data when any of the following conditions are met:

- the employee consents;
- the processing is backed by statutory authority;
- the employer needs to process the data to carry out a contract to which the employee is a party (the employment relationship is considered this type of contract), or to take action before entering the contract, if the employee requests it;
- the processing satisfies the employer’s legal obligation;
- the processing protects the employee’s vital interests;
- the employer needs to process the data to act in the public interest;
- the employer needs to process the data to exercise official authority; or
- the employer, or a third party in receipt of the data, has a legitimate interest protected by the processing that is not outweighed by the employee’s interests.

Sensitive data concerning, for example, an employee’s race, ethnic origin, political opinions, party affiliations or religion, may be processed with employee consent or statutory authority.

Transfer

Employers may send employees’ personal data to countries with “adequate protection” for the data’s security.

Employers may send personal data to countries with inadequate protection if any of the following conditions are met:
the employee consents;

the transfer is required by an international agreement or membership in an international organization;

the transfer is needed to carry out a contract to which the employee is a party (the employment relationship is considered this type of contract), or to take action before entering the contract, if the employee requests it;

the transfer must take place before a contract made with a third party in the employee’s interest is completed;

the transfer protects the employee’s vital interests;

the transfer is needed to make, exercise or defend a legal claim;

the transfer protects an important public interest;

a statutory authority requires the production of data from a public register; or

the transfer is covered by adequate safeguards, such as an intercompany agreement, and has been approved by the Inspectorate, who may stipulate conditions.

**Rights and Responsibilities**

Employers processing personal data must tell employees:

- why the data is being processed;
- if anyone will see the data and, if so, who will see it; and
- that they have the right to see and correct the data.

Employers must notify the Inspectorate before automatically processing employees' personal data or manually processing sensitive data.

Notification will not be required, however, if the employee consents, the data concerns the employment relationship, and the data will be used for human resources/employee administration purposes.

Employers must make sure personal data remains correct and current, and that it is kept only as long as necessary.
# PHILIPPINES

## LAW

The Philippines Constitution and Civil Code establish traditional privacy rights. There is no general law on data privacy; Presidential Decree No. 1718 (P.D. 1718), which applies to data transfers, was passed in 1980 but has no accompanying rules and regulations and never has been strictly enforced. A data privacy law expected to be based on the European Union Data Protection Directive 95/46/EC is being drafted by the Information Technology and E-Commerce Council.

## REGISTRATION

There is no requirement to register or notify the privacy authorities of a database containing information regarding employees.

## COLLECTION AND PROCESSING

No law specifically requires an employee's consent when an employer processes personal data. However, because a data protection law may be enacted soon, employers are advised to disclose personal data processing activities to employees.

## TRANSFER

At this time, no law specifically requires employee consent for the transfer of personal data out of the country, but employers are advised to obtain consent.

In general, P.D. 1718 prevents employers from transferring employee’s personal data out of the country when the transfer negatively affects the interests of Philippine businesses, agencies or individuals.

However, employers may send personal data to another country if any of the following conditions are met:

- the transfer occurs in the regular course of business with a main office, parent company or organization;
- the transfer is needed to make a business proposal;
- the transfer is needed to negotiate or complete a business deal;
- the transfer complies with an international agreement that the Philippines is a party to; or
- the transfer is backed by authority granted by the president or his representatives.

## RIGHTS AND RESPONSIBILITIES

No specific rights and responsibilities.
# Poland

## Law
The Constitution of Poland establishes traditional privacy rights and provides protection for individuals’ personal data. The Law on the Protection of Personal Data Protection brought Polish law into compliance with the EU Data Protection Directive 95/46/EC. It is enforced by the Bureau of Inspector General for Personal Data Protection (the Bureau). Poland joined the European Union in May 2004.

## Registration
In general, databases must be supplied to the Bureau for inclusion in a public register. However, there is no registration requirement when an employer processes personal data relating to employment or services received by the employer.

## Collection and Processing
Employers may process employees’ personal data when any of the following conditions are met:

- the employee consents;
- the employer has a legal right or duty to process the data;
- the employer needs to process the data to carry out a contract to which the employee is a party (the employment relationship is considered this type of contract), or to take action before entering a contract, if the employee requests it;
- the employer needs to process the data to act in the public interest, when stipulated by law; or
- the employer, or a third party in receipt of the data, has a legitimate reason for the processing and it doesn’t violate the employee’s rights and freedoms.

Employers may process sensitive data concerning, for example, an employee’s race, ethnic origin, political opinions, party affiliations or religion, when all of the following conditions are met:

- the employee consents in writing;
- the employer must process the data to meet its employment obligations; and
- the processing is lawful.

## Transfer
In general, employers may send personal data to other countries whose data security protections are at least comparable to Poland’s.

Employers may send personal data to countries that do not have comparable protections if any of the following conditions are met:

- the employee consents in writing;
- the transfer is needed to carry out a contract between the employer and the employee, or the employee requests it;
- the transfer is needed to carry out a contract between the employer and a third party when
the contract serves the employee’s interests;

• the employer needs to make the transfer to establish a legal claim or to serve the public interest;

• the transfer will protect the employee’s vital interests;

• the data is available to the public; or

• the transfer is covered by “standard contractual clauses” or other acceptable means of protecting the employee’s privacy rights and freedoms, and the Bureau has approved it.

### Rights and Responsibilities

<table>
<thead>
<tr>
<th>Rights and Responsibilities</th>
<th>Employers must do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• collect the data for a specific purpose;</td>
</tr>
<tr>
<td></td>
<td>• hold the data only as long as needed;</td>
</tr>
<tr>
<td></td>
<td>• keep the data accurate and up to date;</td>
</tr>
<tr>
<td></td>
<td>• inform the employees why the data is being processed;</td>
</tr>
<tr>
<td></td>
<td>• inform the employees of any third parties that will be receiving the data;</td>
</tr>
<tr>
<td></td>
<td>• keep the data secure and confidential; and</td>
</tr>
<tr>
<td></td>
<td>• give employees access to the data and a chance to correct any mistakes.</td>
</tr>
</tbody>
</table>
PORTUGAL

**LAW**
The Constitution of Portugal establishes traditional privacy rights and protects an individual’s personal data. A member of the European Union, Portugal implemented the EU Data Protection Directive 95/46/EC with the 1998 Act on the Protection of Personal Data (the Act). The Act governs the collection, use and transfer of both manual and electronic personal data. It is enforced by an independent agency, the National Data Protection Commission (DPC).

**REGISTRATION**
Employers must inform the DPC before collecting and processing employees’ personal data, unless any of the following conditions are met:

- the data concerns employees’ salaries or benefits;
- the data is used to figure withholding taxes or social security payments;
- the processing complies with a court ruling or collective agreement;
- the processing determines employees’ profit sharing; or
- the processing is done for statistical purposes related to salaries.

**COLLECTION AND PROCESSING**
Employers may process employees’ personal data when any of the following conditions are met:

- the employee clearly consents;
- the employer needs to process the data to carry out a contract to which the employee is a party (the employment relationship is considered this type of contract), or to take steps before entering a contract or a statement of the employee’s plan to negotiate, if the employee requests it;
- the processing satisfies the employer’s legal obligation;
- the processing protects the employee’s vital interests and the employee is physically or legally unable to consent;
- the processing is necessary to an act in the public interest or to exercise official authority held by the employer or a third party in receipt of the data; or
- the processing serves a legitimate interest of the employer or a third party in receipt of the data, except where the employee’s fundamental rights, freedoms and guarantees take precedence.

Employers generally may not process sensitive data concerning, for example, an employee’s race, ethnic origin, political opinions, party affiliations or religion. Exceptions include when the employee gives explicit consent or when the processing is approved by the DPC.

The DPC favors the use of industry-specific codes of conduct that promote compliance with the Act, and will review codes for conformity with data protection laws and regulations.
| **TRANSFER** | Employers in compliance with the Act may transfer employees' personal data out of Portugal to EU members or non-EU countries with "adequate protection" for the data's security.

The DPC may allow an employer to send personal data to countries inadequate data protection when any of the following conditions are met:

• the employee clearly and explicitly consents;

• the transfer is needed to carry out a contract between the employer and the employee or to take steps before entering a contract if the employee requests it;

• the transfer is needed to carry out a contract made in the interest of the employee between the employer and a third party; or

• the transfer is covered by "standard contractual clauses" or other acceptable means of protecting the employee's privacy rights and freedoms, and the DPC authorizes it.

| **RIGHTS AND RESPONSIBILITIES** | 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 |
**SAUDIA ARABIA**

<table>
<thead>
<tr>
<th><strong>LAW</strong></th>
<th>There is no data privacy law in Saudi Arabia.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>REGISTRATION</strong></td>
<td>There is no requirement to register or notify the privacy authorities of a database containing information regarding employees.</td>
</tr>
<tr>
<td><strong>COLLECTION AND PROCESSING</strong></td>
<td>No law specifically requires an employee’s consent when employers process personal data. However, employers are advised to tell employees about the processing.</td>
</tr>
<tr>
<td><strong>TRANSFER</strong></td>
<td>No law specifically requires an employee’s consent to sending his or her personal data out of the country, but obtaining employee consent is advised.</td>
</tr>
<tr>
<td><strong>RIGHTS AND RESPONSIBILITIES</strong></td>
<td>No specific rights and requirements.</td>
</tr>
</tbody>
</table>
**SINGAPORE**

<table>
<thead>
<tr>
<th><strong>LAW</strong></th>
<th>The Singapore Constitution does not provide a right to privacy for individuals. A proposed general data protection law has been kept “under review” by the government of Singapore for 14 years. However, the common law of confidence protects personal data from being revealed and used without authorization. There are also laws earmarked for certain sectors and codes of practice adopted by some industries. The National Internet Advisory Committee published a voluntary Model Data Protection Code for the Private Sector (Model Code) in February 2002, based on sources that include the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the 1996 Canadian Model Code for the Protection of Personal Information and the EU Data Protection Directive 95/46/EC. Compliance is optional.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>REGISTRATION</strong></td>
<td>There is no requirement to register or notify the privacy authorities of a database containing information regarding employees.</td>
</tr>
<tr>
<td><strong>COLLECTION AND PROCESSING</strong></td>
<td>No law specifically requires an employee’s consent when employers process personal data. Because the Model Code exists and a data protection law may be enacted, employers are advised to disclose personal data processing activities to employees.</td>
</tr>
<tr>
<td><strong>TRANSFER</strong></td>
<td>No law specifically requires an employee’s consent to the transfer of personal data out of the country, but employers are advised to obtain consent.</td>
</tr>
<tr>
<td><strong>RIGHTS AND RESPONSIBILITIES</strong></td>
<td>No specific rights and responsibilities.</td>
</tr>
</tbody>
</table>
The Constitution of Spain establishes traditional privacy rights and protects an individual’s personal data. 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 Act governs public- and private-sector collection, use and transfer of personal data. It is enforced by the Data Protection Agency (DPA).

Before processing personal data, employers are required to register any database with the DPA. Employers must notify the DPA before sending employees' personal data out of the country. The DPA will consider data processing codes of conduct submitted by employers for approval and inclusion in the General Data Protection Register.

Employers may process employees’ personal data when any of the following conditions are met:

- the employee consents;
- the employer needs to process the data to carry out a contract to which the employee is a party (the employment relationship is considered this type of contract), or to take steps before entering a contract, if the employee requests it;
- the processing satisfies a legal obligation;
- the processing protects the employee’s vital interests;
- the processing is needed for a public purpose; or
- the employer has a legitimate reason for the processing (for personnel or human resource purposes, for example), except if the employee’s fundamental rights, freedoms or other legitimate interests would be unreasonably prejudiced.

Employers may process sensitive data concerning, for example, an employee’s race, ethnic origin, political opinions, party affiliations or religion, only when the employee consents or the processing is authorized by law.

Employers may transfer employees’ personal data to EU member states or non-EU countries whose data security protections are at least equal to Spain’s.

- Employers may send personal data to countries that do not have equal protections if any of the following conditions are met:
  - the employee consents;
  - the transfer is needed to carry out a contract between the employer and the employee, or the employee requests it;
  - the transfer is needed to carry out a contract between the employer and a third party when the contract serves the employee’s interests;
• the employer needs to make the transfer to establish a legal claim or to serve the public interest; or

• the transfer is covered by “standard contractual clauses” (the preferred method) or other acceptable means of protecting the employee’s privacy rights, and the DPA Director has approved it.

For transfers of data to the United States, compliance with the US/EU Safe Harbor principles satisfies the requirements of Spain’s transfer law.

<table>
<thead>
<tr>
<th>RIGHTS AND RESPONSIBILITIES</th>
<th>Employers must do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• collect the data for a specific purpose;</td>
</tr>
<tr>
<td></td>
<td>• hold the data only as long as needed;</td>
</tr>
<tr>
<td></td>
<td>• keep the data accurate and up to date;</td>
</tr>
<tr>
<td></td>
<td>• inform the employees why the data is being processed;</td>
</tr>
<tr>
<td></td>
<td>• inform the employees of any third parties that will be receiving the data;</td>
</tr>
<tr>
<td></td>
<td>• keep the data secure and confidential; and</td>
</tr>
<tr>
<td></td>
<td>• give employees access to the data and a chance to correct any mistakes.</td>
</tr>
</tbody>
</table>
## Sweden

### Law

The Constitution of Sweden establishes traditional privacy rights and protects an individual's personal data. A member of the European Union, Sweden implemented the EU Data Protection Directive 95/46/EC with the Personal Data Act 1998 (the Act), which governs personal data processing, and the Personal Data Ordinance 1998, which contains additional regulations. The Act is enforced by the Data Inspection Board (DIB).

### Registration

Employers processing employees' personal data must notify the DIB. Notification is not required if the employer has an independent data protection representative to ensure compliance with the Act.

### Collection and Processing

Employers may process employees' personal data when any of the following conditions are met:

- the employee clearly consents;
- the employer needs to process the data to carry out a contract to which the employee is a party (the employment contract is considered this type of contract), or to take steps before entering a contract, if the employee requests it;
- the processing protects the employee's vital interests; or
- the processing satisfies a legal obligation.

Employers may process sensitive data concerning, for example, an employee’s race, ethnic origin, political opinions, party affiliations or religion, only when a specific exception applies. Examples of exceptions include obtaining explicit consent from the employee or satisfying employment law.

### Transfer

Employers may transfer employee’s personal data to EU member states and non-EU countries with "adequate protection" for the data’s security.

Employers may transfer personal data to countries without "adequate protection" when any of the following conditions are met:

- the employee clearly consents;
- the transfer is needed to carry out a contract to which the employee is a party;
- the transfer is covered by "standard contractual clauses"; or the transfer complies with the US/EU Safe Harbor principles.

### Rights and Responsibilities

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.
SWITZERLAND

**LAW**

The Constitution of Switzerland establishes traditional privacy rights and protects an individual's personal data. Privacy protections also exist in sections of the Civil Code, the Code of Obligations and the Penal Code. The Federal Data Protection Act of 1992 (the Act) governs public- and private-sector personal data processing. The Act is enforced by the Office of the Federal Data Protection Commissioner, which also registers databases in the Register for Data Files. Switzerland's 26 cantons, or states, have additional data protection laws and enforcement commissioners.

**REGISTRATION**

Before processing employees' personal data, employers must register any database with the DPC when it will contain personal profiles or sensitive data (concerning, for example, an employee’s race, ethnic origin, political opinions, party affiliations or religion), or when it will be shared with a third party.

Employers do not need to register a database when employees know about the processing or the processing is required by law.

Employers must notify the DPC before transferring personal data out of the country unless they are legally obligated to make the transfer or the employee knows about it.

**COLLECTION AND PROCESSING**

The Act considers the processing of personal data by an employer to be an unlawful infringement of an employee’s privacy except when one of the following conditions applies:

- the employee consents;
- the processing is necessary to implement the employment agreement;
- the processing serves a compelling public or private interest; or
- the processing is supported by law.

Under the Swiss Code of Obligations, employers may process personal data only if the data applies to an employee's ability to do his or her job, or to the performance of an employment contract.

**TRANSFER**

Employers may send employees’ personal data to countries with data security protections equal to Switzerland’s, as long as the transfer does not seriously harm the employee’s privacy.

The DPC advises that employers use “standard contractual clauses” in transfer agreements to ensure equivalent protection.

Because the European Union has decided that Switzerland provides “adequate protection” for personal data security, transfers of data from EU member states to Switzerland are considered to comply with the EU Data Protection Directive 95/46/EC.
When employees ask, employers must tell them:

- what personal data and categories of data have been recorded in their files;
- why the data was processed;
- the legal basis for the processing, if one was necessary;
- who is processing the data; and
- who will receive the data.

Employers must make sure that employees’ personal data is accurate and that it remains secure and private.

In general, employees have the right to know what personal data is being recorded by their employers.
<table>
<thead>
<tr>
<th><strong>TAIWAN</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LAW</strong></td>
</tr>
<tr>
<td><strong>REGISTRATION</strong></td>
</tr>
<tr>
<td><strong>COLLECTION AND PROCESSING</strong></td>
</tr>
<tr>
<td><strong>TRANSFER</strong></td>
</tr>
<tr>
<td><strong>RIGHTS AND RESPONSIBILITIES</strong></td>
</tr>
</tbody>
</table>
**THAILAND**

<table>
<thead>
<tr>
<th>LAW</th>
<th>Thailand’s 1997 Constitution establishes traditional privacy rights. There is no general data protection law, but the Data Protection and Privacy Bill (the Bill), proposed in 2001, would regulate the private- and public-sector collection, processing, use and transfer of personal data. The Bill requires employers to give notice or get consent from employees either before or as soon as possible after collecting or storing their personal data, and creates a Board of Data Privacy Protection for enforcement. A second draft of the Bill awaits approval by the Thai Cabinet.</th>
</tr>
</thead>
<tbody>
<tr>
<td>REGISTRATION</td>
<td>There is no requirement to register or notify the privacy authorities of a database containing information regarding employees.</td>
</tr>
<tr>
<td>COLLECTION AND PROCESSING</td>
<td>No law specifically requires an employee’s consent when employers process personal data. However, because a data protection law may be enacted soon, employers are advised to disclose data processing activities to employees.</td>
</tr>
<tr>
<td>TRANSFER</td>
<td>No law specifically requires an employee’s consent when sending personal data out of the country. However, because a data protection law may be enacted soon, employers are advised to obtain consent.</td>
</tr>
<tr>
<td>RIGHTS AND RESPONSIBILITIES</td>
<td>No specific rights and responsibilities.</td>
</tr>
</tbody>
</table>
**UNITED KINGDOM**

### LAW

A member of the European Union, the United Kingdom implemented the EU Data Protection Directive 95/46/EC in March 2000 with the Data Protection Act 1998 (the Act). The second of two transitional phase-in periods will end on October 24, 2007, when some kinds of personal data will become fully subject to the Act. Enforcement is through the Office of the Information Commissioner, which published a guide to the Act, the Employment Practices Data Protection Code, in 2005.

### REGISTRATION

Employers processing employees’ personal data must inform the Information Commissioner so the database may be registered and made public in the Register of Data Controllers. Any changes or additions to any entries will require additional notification.

The notification should include the following information:

- what data is being collected;
- why the data will be processed;
- which employees are included; and if applicable, that the data will be transferred outside the European Economic Area.

### COLLECTION AND PROCESSING

Employers may collect and process employees’ personal data when any of the following conditions are met:

- the employee consents;
- the employer needs to process the data to enter into or carry out a contract to which the employee is a party;
- the processing satisfies the employer’s legal obligation;
- the processing protects the employee’s vital interests;
- the processing is required by an enactment, the Crown or the government, or to perform a public function in the public interest, or to administer justice; or
- the employer has a legitimate reason for the processing, except if the employee’s rights, freedoms or other legitimate interests would be damaged.

Employers are required to compile databases only for specific, legal purposes, limit their collection to data relevant to and adequate for those purposes, and use processing methods consistent with those purposes.

### TRANSFER

Employers may send employees’ personal data out of the United Kingdom if any of the following conditions are met:

- the employee consents;
- the transfer is essential to the employment contract;
- the transfer is needed to carry out a contract between the employer and a third party when
the contract serves the employee’s interests;

- the transfer is legally required or essential to an important public interest;
- the transfer protects the employee’s vital interests; or
- the data is public.

Transfer of an employee’s personal data to non-EU/European Economic Area countries is allowed if the countries provide “adequate protection” for the security of the data, or if the transfer is covered by “standard contractual clauses” approved by the United Kingdom or other acceptable non-standard contracts and codes of conduct.

For transfer of data to the United States, compliance with the US/EU Safe Harbor principles satisfies the requirements of the United Kingdom’s transfer law.

<table>
<thead>
<tr>
<th>RIGHTS AND RESPONSIBILITIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employers must do the following:</td>
</tr>
<tr>
<td>• collect the data for a specific purpose;</td>
</tr>
<tr>
<td>• hold the data only as long as needed;</td>
</tr>
<tr>
<td>• keep the data accurate and up to date;</td>
</tr>
<tr>
<td>• inform the employees why the data is being processed;</td>
</tr>
<tr>
<td>• inform the employees of any third parties that will be receiving the data;</td>
</tr>
<tr>
<td>• keep the data secure and confidential; and</td>
</tr>
<tr>
<td>• give employees access to the data and a chance to correct any mistakes.</td>
</tr>
</tbody>
</table>
For more Information
If you have questions about the design, implementation and maintenance of employee stock purchase rights in any country, please contact:

Dean Fealk
T +1 415 836 2521
F +1 415 659 7421
dean.fealk@dlapiper.com

DLA Piper
555 Mission Street
Suite 2400
San Francisco, CA 94105

www.dlapiper.com

* Includes DLA Piper Offices, DLA Piper Group Firms and DLA Piper Focus Firms