

A Regional Guide to Employee Data Privacy

ASIA

理慈

Lee, Tsai & Partners

A GREATER CHINA LOCAL FIRM

Introduction

Data privacy is a priority for all employers but especially those with operations in more than one country. It impacts all aspects of the employment relationship and, with the increase in data transfers between businesses and across borders, employers often need to comply with multiple laws to minimize the risk of significant fines and liabilities.

A Regional Guide to Employee Data Privacy is designed to help employers navigate the specific, and increasing, challenges of handling employee data in different jurisdictions. Covering 18 key countries, the guide contains the following:

- **Key Questions & Answers** – covering applicant and employee personal data, privacy statements and policies, retention periods for employee data, transfers of employee data overseas and to third parties, sanctions for breach and potential pitfalls for employers; and
- **“In Brief” and “In Detail” Guidance** – providing both quick reference and more detailed content across all jurisdictions.

We hope that you will find this publication useful. It has been compiled by lawyers from a major international law firm as well as partner law firms in other jurisdictions.

USER GUIDE



HOME



COUNTRIES

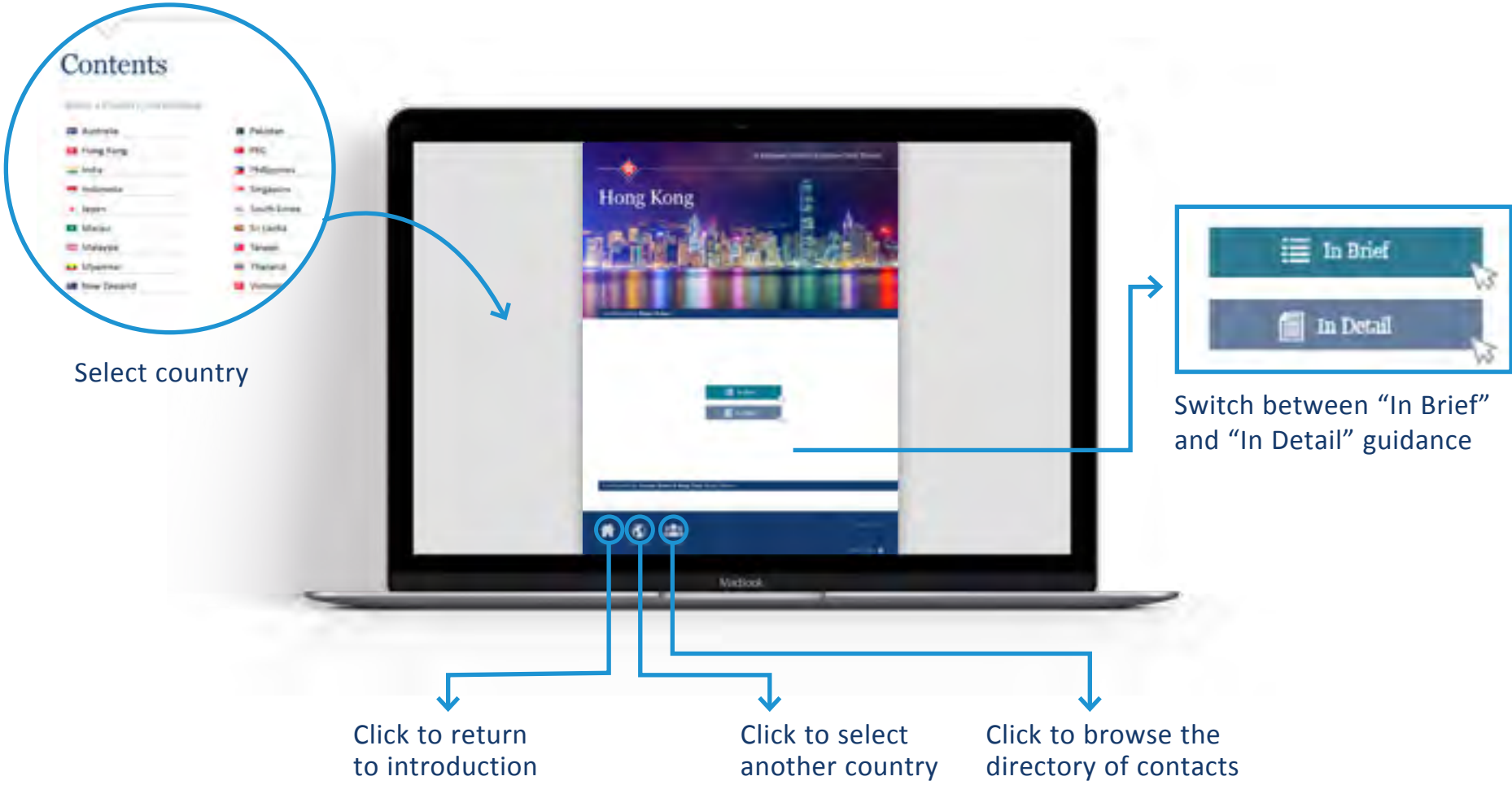


DIRECTORY

August 2018

SCROLL DOWN

User Guide



Contents

Select a Country/Jurisdiction

-  Australia
-  Hong Kong
-  India
-  Indonesia
-  Japan
-  Macau
-  Malaysia
-  Myanmar
-  New Zealand

-  Pakistan
-  PRC
-  Philippines
-  Singapore
-  South Korea
-  Sri Lanka
-  Taiwan
-  Thailand
-  Vietnam



Australia



Contributed by: **Corrs Chambers Westgarth**



In Brief



In Detail

Contributed by: **John Tuck and Anthony Forsyth**, Corrs Chambers Westgarth



[Link to biography >](#)



[Link to biography >](#)



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



Australia

In Brief

1. Is there a law regulating applicant personal data?

The personal information of job applicants, including information contained in CVs, references and background checks, must be dealt with in accordance with the Privacy Act 1988 (Cth) (the “**Privacy Act**”).

2. Is there a law regulating employee personal data?

Yes, the Privacy Act is the principal relevant legislation, although for private sector entities it provides an exemption in respect of specified “employee records.”

3. Do I need to have a privacy statement or agreement?

There is no legal requirement for such a statement or agreement; however, federal legislation requires certain organizations to have a clearly expressed and up-to-date privacy policy.

4. How long must I retain employee data? What is best practice?

Various state and federal statutes require certain employee records (which could include personal data) to be retained for specified periods. For example, the Fair Work Act 2009 (Cth) and regulations made under that legislation require that certain employee records be kept for at least seven years.

5. Can I transfer employee data overseas?

Yes, subject to Australian Privacy Principle 8.

6. Can I transfer employee data to a third party?

Yes, subject to the Privacy Act and Australian Privacy Principles 3, 5 and 6.

7. What are the consequences of breach?

A determination may be made by the Australian Information Commissioner, including a declaration that a reasonable act should be performed to redress any loss or damage suffered by a complainant, or that a complainant is entitled to a specified amount of compensation for any loss or damage suffered (including injury to feelings or humiliation).

Determinations may be enforced by proceedings commenced in the Federal Court or Federal Circuit Court. The Court may make such orders as it thinks fit.

8. What are the main pitfalls?

Pitfalls include:

- (a) assuming privacy regulation is the same across all jurisdictions;
- (b) failure to ensure that any records held containing the personal information of employees are only dealt with in a manner that directly relates to the employment relationship; that is, any employee records should only be collected, used and disclosed for the purpose of the employment relationship;
- (c) collection of unnecessary personal information and consequent exposure to legal risk; and
- (d) failure to develop, implement and enforce comprehensive policies and procedures around the handling of personal information.





Australia

In Detail

1. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant’s personal data in your jurisdiction?

It has been assumed for the purposes of this Australian chapter that the reference to “personal data” has the same or a similar meaning as the term “personal information” under the Privacy Act 1988 (“**Privacy Act**”). Privacy issues also arise from the undertaking of workplace surveillance and monitoring, which are the subject of federal, state and territory legislation, but this has not been covered in this chapter.

As explained in detail in our response to question 2 below, the Privacy Act regulates the use, storage, handling, access, disclosure and security of personal information by particular Australian government agencies and private sector organizations.

An “employee records” exemption provides that rights and obligations arising under the Privacy Act do not apply to certain acts or practices. However, this exemption only applies if an employer’s act or practice is directly related to a current or former relationship between the employer and the individual, and an employee record held by the organization relating to the individual.

Therefore, the exemption does not apply to the collection of personal information about *prospective* employees. The personal information of job applicants, including information contained in CVs, references and background checks, must be dealt with in accordance with the Privacy Act. For example, personal information may only be collected where it is necessary for one or more of the legitimate functions or activities of the business, and must only be used for the purpose for which it is collected.

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee’s personal data in your jurisdiction?

Privacy in the employment context usually concerns the use by an employer of personal information about an employee, including information about the employee’s health and fitness.

In Australia, legal obligations in respect of privacy of personal information are largely derived from statute. There is no “constitutional” protection of privacy rights similar to that which exists in other jurisdictions such as the United States.





Australia

In Detail

Privacy in Australia is regulated at both the Federal and State level. Therefore, privacy obligations differ across the various jurisdictions, as well as between the public and private sectors. In each Australian jurisdiction, privacy of personal information may be regulated by specific privacy legislation and also by legislation in respect of health records, freedom of information and electronic surveillance.

A summary of some of the key legislation that regulates privacy in Australia is set out below.

Privacy Act 1988 (Cth)

The Privacy Act regulates the use, storage, handling, access, disclosure and security of personal information by Australian Government agencies, and Australian private sector and not-for-profit organizations with an annual turnover greater than AUD 3 million.

There are some smaller businesses which may have an annual turnover of less than AUD 3 million whose activities are regulated by the Privacy Act. This includes private sector health service providers or businesses that trade in personal information.

The Privacy Act is intended to protect “personal information” about individuals who can reasonably be identified from the information. The legislation defines personal information as: *“information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not”*. This would include, for example, a person’s name, address, phone number, date of birth and medical records (see Australian Government, Office of the Australian Information Commissioner, *Privacy Act*, at: <https://oaic.gov.au/privacy-law/privacy-act/>).

The Privacy Act establishes 13 Australian Privacy Principles that (together) operate to regulate the use, storage, handling, access and security of personal information by organizations subject to the legislation. Organizations may discharge their obligations by creating and complying with a code of practice tailored to the organization, and approved for use by the Australian Information Commissioner.

As indicated above, the Privacy Act expressly excludes acts done, or practices engaged in, by an employer (covered by the Privacy Act) in respect of an individual, if the act or practice is directly related to a current or former employment relationship between the employer and the individual and an “employee record” held by the organization and relating





Australia

In Detail

to the individual. “Employee records” are defined as a record of personal information relating to the employment of the employee. Examples of personal information relating to the employment of the employee are health information about the employee, and personal information about any or all of the following:

- (a) the engagement, training, disciplining or resignation of the employee;
- (b) the termination of the employment of the employee;
- (c) the terms and conditions of employment of the employee;
- (d) the employee’s personal and emergency contact details;
- (e) the employee’s performance or conduct;
- (f) the employee’s hours of employment;
- (g) the employee’s salary or wages;
- (h) the employee’s membership of a professional or trade association;
- (i) the employee’s trade union membership;
- (j) the employee’s recreation, long service, sick, personal, maternity, paternity or other leave; and
- (k) the employee’s taxation, banking or superannuation affairs.

Practically, this means an employer does not need to comply with the Australian Privacy Principles (for example, in relation to storage, access, use, disclosure and handling of the information) in relation to records about its employees that fall within the above definition.

It is important to note that the employee records exemption relates to private sector organizations only. This means that Australian government employee records must be dealt with in accordance with the Privacy Act.

The existence of the “employee records” exemption does not mean that all activities of an employer that relate to employment are excluded. For example, as indicated in our response in question 1 above, a prospective employee does





Australia

In Detail

not have an employment relationship with the potential employer. Therefore, potential employers and/or recruitment agencies must comply with the obligations of the Privacy Act in respect of candidates for employment.

Another limitation to the exemption is that it will no longer apply once an employer discloses the employee records to a third party that is not involved in the employment relationship, as this falls outside the scope of the employment relationship.

Fair Work Act 2009 (Cth)

The Fair Work Act 2009 (Cth) ("**Fair Work Act**") regulates the employment relationship between employees and "national system employers". A "national system employer" is broadly defined in the Fair Work Act and relevantly includes all incorporated employers and, subject to the location in which the employment is based, various other employers in Australia.

Privacy rights under the Fair Work Act arise insofar as unions have certain rights to access employment records in respect of their members. In some cases a non-member's record can be accessed, particularly in circumstances where the non-member consents or the Fair Work Commission makes an order granting access.

It is important to note that unions that access employee records must then comply with the obligations set out in the Privacy Act in respect of those records. Further, the employee records exemption will not apply in respect of the union's management of those records. Accordingly, unions accessing employee records pursuant to their rights under the Fair Work Act will be required to comply with the privacy obligations under the Privacy Act in respect of those records.

State and Territory privacy legislation

In most States and Territories, privacy regulation is limited to the public sector. Employers should be mindful of the following legislation:

- (a) Victoria - Privacy and Data Protection Act 2014 (Vic) and the Charter of Human Rights and Responsibilities Act 2006 (Vic);
- (b) New South Wales - Privacy and Personal Information Protection Act 1998 (NSW);
- (c) Queensland - Information Privacy Act 2009 (Old);





Australia

In Detail

- (d) Western Australia - Freedom of Information Act 1992 (WA);
- (e) South Australia - Information Privacy Principles (IPPs) reissued by the State Government of South Australia in 1992;
- (f) Tasmania - Personal Information and Protection Act 2004 (Tas);
- (g) Northern Territory - Information Act (NT); and
- (h) Australian Capital Territory - Information Privacy Act 2014 (ACT).

There is also State legislation regulating privacy in respect of health records. For example, the Health Records and Information Privacy Act 2002 (NSW) regulates the use and handling of health information by public and private sector health service providers and other organizations that collect, hold or use health information (see Information and Privacy Commission New South Wales, HRIP Act, at: <https://www.ipc.nsw.gov.au/hrip-act>). See further our response to question 6 below.

Freedom of information legislation

The Freedom of Information Act 1982 (Cth) provides that every person has a right to access documents held by federal government agencies or Ministers, other than exempt documents. One of the classes of exempt documents is where the disclosure of the document would involve the unreasonable disclosure of “personal information” of any person other than the applicant who has made the request. A number of factors will be taken into account in determining whether the disclosure would be “unreasonable.”

Each State and Territory also has legislation dealing with freedom of information.

3. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee’s personal data?

There is no specific legal requirement to have a document to deal with employees’ personal data in particular.

However, Australian Privacy Principle 1 stipulates that organizations covered by the Privacy Act must have a clearly expressed and up-to-date privacy policy about the management of personal information by the organization.





Australia

In Detail

Such a policy must contain the following information:

- (a) the kinds of personal information the organization collects and holds;
- (b) how the organization holds that information;
- (c) the purposes for which the organization collects, holds, uses and discloses the information;
- (d) how an individual may access their personal information held by the organization or seek the correction of the information;
- (e) how an individual may complain about a breach of the Australian Privacy Principles and how the organization will deal with a complaint; and
- (f) whether the organization is likely to disclose information to overseas recipients and, if so, the countries to which the information will be disclosed (if this is practicable to specify).

Further, as indicated in our response in question 2 above, organizations may discharge their privacy obligations by creating and complying with a code of practice tailored to the organization and approved for use by the Australian Information Commissioner.

Policies and procedures will be particularly important in circumstances where it is not clear whether employee records are being collected, used or disclosed for the purpose of the employment relationship. For example, employers should obtain written consent from prospective employees in relation to the collection, use and disclosure of personal and sensitive information that is obtained during the recruitment process (for example, by indicating consent in a written application form or through online application procedures).

4. For how long must an employer retain an employee's personal data? What is best practice?

Provided that the personal data falls within the employee records exemption under the Privacy Act, there are no obligations with respect to the retention of personal data under the legislation.

However, various Federal and State legislation require that employers retain certain records relating to employees (which could include personal data). The Fair Work Regulations 2009 (Cth) require that specific employee records be retained for all employees (with certain limited exceptions) for a period of seven years.





Australia

In Detail

For the purposes of the Fair Work Regulations, “record” means any record about the employee (or former employee) containing information about the nature of their employment and their entitlements (e.g., applicable industrial instruments, classification, pay rates, hours, shift work, overtime, leave, superannuation, etc.), and also information about the employee’s termination (if a former employee). However, the Fair Work Regulations do not require that employers keep records relating to an employee’s performance.

The Fair Work Regulations stipulate that records must be kept in a legible form in the English language and in a form that is readily accessible to a Fair Work Inspector. Importantly, the Fair Work Regulations do not stipulate that the record must be an original copy or kept in hard copy.

The Superannuation Guarantee (Administration) Act 1992 (Cth) requires corporations to retain specific superannuation documents for a period of five years. Further, the Income Tax Assessment Act 1997 (Cth) requires that specific taxation records must be retained for five years.

Obligations in relation to employee records also arise under workers’ compensation legislation in each of the States and Territories. For example, in NSW employers are required under the Workers Compensation Act 1987 (NSW) to retain wages “records” (which may include personal data) for at least five years.

Finally, it is important to note that where litigation is anticipated or has been commenced, an employer must not destroy or dispose of any documents that may be required for the purposes of the litigation (which may include employee records).

5. What are the legal restrictions on transferring employees’ personal data outside your jurisdiction?

“Cross-border disclosure” of personal information is the subject of a specific Australian Privacy Principle referring to the movement of personal data across national borders.

The Privacy Act originally dealt only with personal information collected and handled within Australia. However, it has since been amended to apply to acts done, or practices engaged in, by an organization outside Australia and the external Territories. The purpose of these amendments to the Privacy Act was to prevent organizations from avoiding their privacy obligations by transferring the handling of personal information to countries with lower privacy protection standards.





Australia

In Detail

Under Australian Privacy Principle 8, an organization in Australia can only transfer personal information outside Australia if:

- (a) the organization reasonably believes that an enforceable law or binding scheme applies at the destination that has the effect of protecting the information in a manner that is substantially similar to the Australian Privacy Principles;
- (b) the individual gives informed consent to the transfer;
- (c) the disclosure of the information is required or authorized by an Australian law or a court or tribunal order;
- (d) a “permitted general situation” exists in relation to the disclosure, for example, where it is unreasonable or impractical to obtain the individual’s consent and the organization reasonably believes the disclosure is necessary to lessen or prevent a serious threat to health or safety;
- (e) in the case of an agency, the disclosure is required or authorized by an international agreement to which Australia is a party; or
- (f) in the case of an agency, the agency reasonably believes the disclosure is necessary for enforcement related activities.

The Australian Information Commissioner has powers to oversee complaints that arise in respect of a breach that occurs outside of Australia and that falls within the scope of the Privacy Act.

6. What are the legal restrictions on transferring employees’ personal data to a third party?

As set out in our response in question 2 above, the obligations set out in the Privacy Act do not apply to the collection, use, disclosure and storage of personal information contained within an employee record, provided that the act or practice directly relates to the employment relationship.

Unfortunately, “directly related” is not defined in the Privacy Act and case law provides little insight into the meaning of “directly related to the employment relationship” in a privacy context. However, an act that may not be “directly related” to the employment relationship may include sending a list of employee details to another organization for marketing purposes.





Australia

In Detail

If an employer that is an organization covered by the Privacy Act seeks to collect, use or disclose employee records in a way not directly related to the employment relationship, it must comply with the Australian Privacy Principles. We set out the key aspects of Australian Privacy Principles 3, 5 and 6 below.

Australian Privacy Principle 3 – Collection of solicited personal information

An organization must only collect personal information that is necessary for one or more of its legitimate functions or activities (the primary purpose). An organization must only collect personal information by lawful and fair means and not in an unreasonably intrusive way. An organization may only collect sensitive personal information about an individual from someone other than the individual if the individual consents, or if the organization is required or authorized by law to collect the information from someone else. Where practicable, however, an organization should collect personal information directly from the individual.

Australian Privacy Principle 5 – Notification of collection of personal information

At the time of collection (or as soon as practicable afterwards) an organization must take reasonable steps to ensure that the individual is told:

- (a) the identity of the organization and how to contact it;
- (b) that the organization has collected the information and the circumstances of that collection;
- (c) that the collection is required or authorized by an Australian law or court or tribunal order, including the name of the law or details of the order;
- (d) the purposes for which the information is collected;
- (e) the main consequences (if any) for the individual if all or some of the information is not collected;
- (f) any other organizations to which the organization usually discloses personal information of the kind collected;
- (g) that the organization’s privacy policy contains information about how the individual may access the information and seek correction of it, or how a complaint about the Australian Privacy Principles or any code binding the organization may be made, and how the organization will deal with such complaints; and





Australia

In Detail

(h) whether the organization is likely to disclose the information to overseas recipients, and if so, the countries to which the information is likely to be disclosed (if this is practicable to specify).

Australian Privacy Principle 6 - Use or disclosure of personal information

As a general rule, an organization should only use or disclose personal information for the purpose for which it was collected (the primary purpose). However, an organization can use or disclose personal information about an individual for another purpose (the secondary purpose) if, among other things:

- (a) the individual has consented; or
- (b) the secondary purpose is related to the primary purpose and the individual would reasonably expect the information to be used or disclosed for the secondary purpose.

Special additional provisions apply for direct marketing and sensitive information (including health information).

Legislation in the Australian Capital Territory, New South Wales and Victoria regulates organizations that collect, hold and use “health information”. Such legislation contains “health record privacy principles” that are broadly similar to the Australian Privacy Principles. In certain circumstances, if the employer collects health information, the employer will be required to comply with the health records legislation in the relevant State or Territory.

7. What are the consequences of breaching privacy laws in your jurisdiction?

General

If an organization breaches an Australian Privacy Principle, the organization will have contravened section 15 of the Privacy Act and interfered with the privacy of an individual contrary to section 13(1)(a) of the Privacy Act.

Individuals must make any complaints regarding an interference with privacy to the relevant organization. If the complaint is not resolved, it can be referred to the Office of the Australian Information Commissioner for conciliation, and if this is not successful, for formal determination (enforceable by the Federal Circuit Court or Federal Court of Australia).





Australia

In Detail

Functions of the Information Commissioner

(a) Powers without complaint

Under section 40(2) of the Privacy Act, the Information Commissioner has the power to investigate an act or practice of an organization that may be an interference with the privacy of an individual or a breach of Australian Privacy Principle 1. If the Commissioner considers it appropriate to do so, the Commissioner may attempt, by conciliation, to effect a settlement of the matters that gave rise to the investigation.

Where the Commissioner has investigated an act or practice (without a complaint having been made under section 36 of the Privacy Act), the Commissioner must report to the Minister about the act or practice if the Commissioner thinks the act or practice is an interference with the privacy of an individual, and does not consider it reasonably possible that the matter giving rise to the investigation can be successfully conciliated. The Minister must table the report before each house of the Federal Parliament. In this way, the report acts to “name and shame” contraveners of Privacy Act obligations.

(b) Powers following complaint

Pursuant to section 40(1) of the Privacy Act, the Information Commissioner must investigate an act or practice if:

- (i) the act or practice may be an interference with the privacy of an individual; and
- (ii) a complaint about the act or practice has been made under section 36 of the Privacy Act.

Pursuant to section 44 of the Privacy Act, if the Commissioner has reason to believe that a person has information or a document relevant to an investigation, the Commissioner may give to the person a written notice requiring the person to give the information to the Commissioner in writing and/or to produce the document to the Commissioner.

The Commissioner is also empowered under sections 45 and 46 to examine witnesses and direct persons to attend compulsory conferences for the purpose of an investigation.





Australia

In Detail

After investigating a complaint, the Commissioner may, under section 52 of the Privacy Act, find the complaint substantiated and make a determination, including a declaration that:

- (i) the respondent has engaged in conduct constituting an interference with the privacy of an individual and must not repeat or continue such conduct;
- (ii) the respondent must take specified steps within a specified period to ensure that such conduct is not continued or repeated;
- (iii) the respondent should perform any reasonable act or course of conduct to redress any loss or damage suffered by the complainant;
- (iv) the complainant is entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice the subject of the complaint; or
- (v) it would be inappropriate for any further action to be taken in the matter.

A determination by the Commissioner is not binding or conclusive between any of the parties to the determination.

An organization that is the respondent to a determination made under section 52:

- (i) must not repeat or continue conduct that is covered by a declaration that determined the respondent had engaged in conduct constituting an interference with the privacy of an individual and should not repeat or continue such conduct;
- (ii) must take the steps specified by a declaration that determined the respondent should perform specified steps within a specified period to ensure the conduct is not continued or repeated; and
- (iii) must perform the act or course of conduct that is covered by a declaration that determined the respondent should perform any reasonable act or course of conduct to redress any loss or damage suffered by the complainant.

The complainant or the Commissioner (if a determination was made under section 52) may commence proceedings in the Federal Court or the Federal Circuit Court for an order to enforce a determination (under section 55A).





Australia

In Detail

If the court is satisfied that the respondent has engaged in conduct that constitutes an interference with the privacy of the complainant, the court may make such orders (including a declaration of right) as it thinks fit.

The court may, if it thinks fit, grant an interim injunction pending the determination of the proceedings.

8. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee's personal data?

Employers should be mindful to ensure that any records held that contain the personal information of employees are only dealt with in a manner that directly relates to the employment relationship. That is, any employee records should only be collected, used and disclosed for the purpose of the employment relationship.

Employers should obtain written consent from prospective employees in relation to the collection, use and disclosure of personal and sensitive information that is obtained during the recruitment process. Employers should consider including such consents in their contracts of employment. Such consents will reduce the likelihood of an employer inadvertently breaching the Privacy Act in relation to information that does not directly relate to the employment relationship.

Broadly speaking, employers should also ensure that they:

- (a) understand the applicable legislation regulating the collection and use of personal information as well as access to personal information;
- (b) do not assume regulation of privacy in Australia is the same across all jurisdictions;
- (c) develop and implement comprehensive policies and procedures regulating the collection, use, handling and storage of personal information in accordance with the Australian Privacy Principles; and
- (d) train employees in the use and handling of personal information in accordance with the law.

Contributed by: **John Tuck and Anthony Forsyth**, Corrs Chambers Westgarth



[Link to biography >](#)



[Link to biography >](#)



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Hong Kong



Contributed by: **Mayer Brown**



In Brief



In Detail

Contributed by: **Duncan Abate & Hong Tran**, Mayer Brown



[Link to biography >](#)



[Link to biography >](#)



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



Hong Kong

In Brief

1. Is there a law regulating applicant personal data?

Yes. Personal Data (Privacy) Ordinance.

2. Is there a law regulating employee personal data?

Yes. Personal Data (Privacy) Ordinance.

3. Do I need to have a privacy statement or agreement?

No particular form of document is needed. Certain information required to be provided by legislation is typically provided in a Personal Information Collection Statement (“PICS”).

4. How long must I retain employee data? What is best practice?

The Employment Ordinance requires certain employee data to be retained for at least 12 months. Best practice suggests two years for recruitment data and seven years for employment data, unless the employer has a legitimate reason for retaining the data for longer (e.g., litigation).

5. Can I transfer employee data overseas?

Yes, subject to certain requirements.

6. Can I transfer employee data to a third party?

Yes, subject to certain requirements.

7. What are the consequences of breach?

- Investigation by Commissioner.
- Commissioner may issue an enforcement notice.
- Criminal liability if failure to comply with an enforcement notice; on first conviction a fine at level 5 (currently HKD 50,000) and imprisonment for two years and, if a continuing offense, a daily penalty of HKD 1,000; on second or subsequent conviction a fine at level 6 (currently HKD 100,000) and imprisonment for two years and, in the case of continuing offense, a daily penalty of HKD 2,000.
- Civil liability: the data subject may claim compensation.

8. What are the main pitfalls?

- Employers should issue PICS and ensure the purpose of use of data specified in PICS covers employers’ requirements.
- Applicants/employees can access and obtain their personal data by serving a Data Access Request (“DAR”). An employer must provide all personal data of the applicant/employee in response to a DAR unless an exception applies (e.g., an employee is using a DAR to “fish” for claims against an employer).



Hong Kong

In Detail

1. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant’s personal data in your jurisdiction?

Yes. In Hong Kong, the Personal Data (Privacy) Ordinance (“**PDPO**”) (which was passed in December 1996) regulates, among other things, the collection, holding, use, security, access and correction of personal data of an individual.

“Personal data” is defined in the PDPO as any data:

- relating directly or indirectly to a living individual (e.g., an applicant or employee);
- from which it is practicable for the identity of the individual to be directly or indirectly ascertainable; and
- that are in a form in which access to or processing of the data is practicable.

Section 4 of the PDPO states that “a data user shall not do an act or engage in a practice that contravenes a data protection principle unless the act or practice, as the case may be, is required or permitted under this Ordinance.” There are six data protection principles (“**DPP**”) with which data users (e.g., employers) are required to comply covering the following areas:

- DPP 1 - purpose and manner of collection of personal data
- DPP 2 - accuracy and duration of retention of personal data
- DPP 3 - use of personal data
- DPP 4 - security of personal data
- DPP 5 - information to be generally available
- DPP 6 - access to personal data

“Data user” is defined as “the person who, either jointly or in common with other persons, controls the collection, holding, processing or use of the personal data” (e.g., an employer). “Data subject” is basically the individual who is the subject of the data (e.g., the applicant or employee).





Hong Kong

In Detail

The Commissioner for Personal Data Privacy (the “**Commissioner**”) has issued a Code of Practice on Human Resource Management (the “**Code**”) in accordance with his powers under the PDPO. The Code came into effect on April 1, 2001 and provides employers with a practical guide to the application of the provisions of the PDPO to employment-related personal data privacy. Where a data user (e.g., an employer) fails to comply with the Code, a court or the Administrative Appeals Board is entitled to take that fact into account when deciding whether there has been a breach of the PDPO. Noncompliance with the Code would also weigh against the party concerned in any case under investigation by the Commissioner.

An employer must comply with each of the DPPs during the recruitment process. For example, the employer must comply with DPP 1 by taking all practical steps to notify job applicants of certain information on or before the collection and use of his/her personal data (for details, please see question 3 below).

Without prejudice to the generality of the DPPs, the Code also provides practical guidance for employers in relation to collecting and handling job applicants’ personal data during the recruitment process. For example:

- An employer should not collect personal data from job applicants unless the purpose for which the data are to be used is lawful (e.g., collecting certain data to unlawfully discriminate against a job applicant is not only contrary to the anti-discrimination ordinances but also DPP 1).
- An employer should not collect personal data from job applicants unless the data are adequate but not excessive in relation to the purpose of recruitment (e.g., obtaining a job applicant’s marital status may be excessive if marital status is irrelevant to the particular job requirements).
- An employer may retain the personal data of a job applicant, whose data are collected during the course of a recruitment exercise, for use in a later exercise of this nature, provided that (i) the employer has a general policy to retain the data for such a purpose, (ii) the employer has a stipulated retention period for keeping such data and (iii) the applicant has not otherwise objected to the use of his/her data for such a purpose. As a matter of good practice, an employer should take steps to inform job applicants about its retention policy of personal data collected in the course of a recruitment exercise. Again, best practice suggests the retention period for recruitment data should not be longer than two years, unless the employer has a legitimate reason for retaining the data for longer (e.g., litigation). It should also provide an opportunity for unsuccessful applicants to request the destruction of the data if the applicant does not wish the data to be used for a subsequent recruitment exercise.





Hong Kong

In Detail

- An employer should take all practicable steps to ensure that, having regard to their confidential nature, the personal data of job applicants are collected, processed and stored securely, irrespective of whether the data are stored in electronic, photographic or hard copy format.
- An employer who wishes to obtain references from a potential candidate’s current or former employers or other sources should ensure that such references are provided with the consent of the candidate concerned.
- Where an employer advertises a vacancy in a vacancy notice that directly solicits the submission of personal data by job applicants, it should ensure that the Personal Information Collection Statement (“**PICS**”) notification requirement (described in question 3 below) is complied with in the advertisement unless (i) the advertisement invites job applicants to respond by filling in a job application form specified by the employer that contains a PICS or (ii) the advertisement expressly identifies the contact person from whom applicants may obtain a copy of the PICS.
- An employer should also comply with (i) the Code of Practice on the Identity Card Number and Other Personal Identifiers (the “**ID Code**”) in assessing whether it is appropriate to collect job applicants’ ID card number or ID card copy and (ii) the Guidance on Personal Data Protection in Cross-border Data Transfer (the “**Cross-border Transfer Guidance**”) if it may involve transferring job applicants’ personal data out of Hong Kong.

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee’s personal data in your jurisdiction?

Yes. The PDPO and the Code, described in question 1 above, also regulate the collection, use and/or handling of an employee’s personal data. An employer should also comply with the ID Code and the Cross-border Transfer Guidance in the collection, using and/or handling of an employee’s personal data.

In addition to the PDPO and the Code, the Commissioner has issued the “Privacy Guidelines: Monitoring and Personal Data Privacy at Work,” which provides practical guidance on personal data privacy where employee monitoring is carried out at work resulting in the collection of personal data of employees through telephone monitoring, email monitoring, internet monitoring and video monitoring.





Hong Kong

In Detail

3. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee’s personal data?

There is no legal requirement under the PDPO for an employer to provide any particular form of document to an employee before the collection of personal data from an individual. However, there are obligations on an employer to take all practical steps to notify a relevant individual (e.g., job applicant or employee) of certain information on or before the collection and use of the individual’s employment-related personal data. This information includes:

- (a) the purpose for which the data are to be used;
- (b) the classes of persons to whom the data may be transferred;
- (c) whether it is obligatory or voluntary for the individual to supply the data unless this is obvious from the circumstances; and
- (d) (before the use of the personal data) details of the rights of the individual to request access to, and correction of, his/her personal data and the name and address of the person to whom such request may be made.

The above information is typically set out in a PICS. Indeed, the Commissioner recommends as a matter of good practice that each employer provides a PICS complying with the notification obligations under the PDPO to each job applicant and employee. The PICS may be attached to, for example, a job application form or incorporated into the body of the job application form itself.

4. For how long must an employer retain an employee’s personal data? What is best practice?

The Employment Ordinance (“EO”) provides that an employer must keep and maintain a “record” setting out the wage and employment history of each employee covering the period of employment during the preceding 12 months. The EO defines a “record” to include particulars in relation to each employee of that employee’s:

- name and identity card number;
- commencement date of employment;
- job title;





Hong Kong

In Detail

- wages paid in respect of each wage period;
- wage period;
- periods of annual leave (including periods of closure of business or part thereof for the purpose of granting any annual leave), sick leave, maternity leave and holidays to which the employee is entitled and that has been taken, together with details of payments made in respect of such periods;
- amount of any end of year payment payable under the EO and the period to which it relates;
- period of notice required for termination of contract; and
- date of termination of employment.

The wage record must be kept at the employer’s place of business or at the place where the employee is employed and for a period of 12 months after the employee ceases to be employed.

The PDPO provides that only data necessary for an employer to fulfill its contractual and legal obligations should be retained and that personal data shall not be kept longer than is necessary for the fulfillment of the purpose (including any directly related purpose) for which the data are to be used.

As discussed above, the “record” required to be retained by the EO must be retained for at least 12 months after the employee ceases to be employed. However, in practice, an employer may need to retain certain employee data longer than 12 months because of, for example, the need to respond to a discrimination complaint, which has a two-year limitation period from the date of the alleged discrimination for commencing court proceedings. In these circumstances, an employer may wish to adopt the following best practice guidelines (which reflect the recommendation of the Code) in relation to the period of document retention:

- (i) two years in respect of recruitment-related data held about a job applicant from the date of rejecting the applicant; and
- (ii) seven years in respect of employment-related data held about an employee from the date the employee leaves employment;

unless





Hong Kong

In Detail

- (iii) the individual concerned has given express consent for the data to be retained for a longer period; or
- (iv) there is a subsisting reason that obliges the employer to retain the data for a longer period. A subsisting reason may be where there is ongoing litigation, where there are contractual obligations on the employer to retain the data or where it is in the public interest (including historical interest) for the data not to be erased.

5. What are the legal restrictions on transferring employees’ personal data outside your jurisdiction?

An employer must comply with the DPPs when transferring employees’ personal data outside Hong Kong. Employment-related personal data may be transferred outside Hong Kong to, say, an associate of the employer, without seeking the relevant employee’s consent, provided that (among other things) such transfer is for (a) a purpose for which the data were to be used at the time of collection of the data or (b) a purpose directly related to the purpose mentioned in (a). To the extent that the overseas entity may be collecting personal data and is subject to the PDPO, such collection of the data must be adequate but not excessive in relation to the purpose for which the data are collected.

Section 33 of the PDPO contains a prohibition against the transfer of personal data to a place outside Hong Kong except in specified circumstances. However, s.33 has not been gazetted to commence. That said, an employer should still ensure it complies with the Cross-border Transfer Guidance as a matter of good practice.

6. What are the legal restrictions on transferring employees’ personal data to a third party?

An employer must comply with the DPPs when transferring employees’ personal data to a third party. Among other things, the employer should comply with DPP 3 and ensure that the transfer to the third party falls within the purpose for which the data was collected. The Code recommends that, if an employer is required to transfer personal data to a third party (e.g., legal representative or HR consultant), the employer should ensure that the data being transferred is limited to the data required for the specific services requested from the third party.

7. What are the consequences of breaching privacy laws in your jurisdiction?

- Data subject may make a complaint: A disgruntled employee may make a “complaint” to the Commissioner. After receiving a complaint and verifying the identity of the complainant, the Commissioner will liaise with the complainant and the party complained against to determine whether on the face of things a case can be established. If so, the Commissioner may try to resolve the dispute through mediation.





Hong Kong

In Detail

- Investigation by Commissioner: If the dispute cannot be resolved by mediation, the Commissioner may carry out a formal investigation. If the issue complained about is serious, the Commissioner may skip the mediation process and go straight to an investigation. If the investigation confirms a contravention of the PDPO, the Commissioner may serve an enforcement notice, which will set out steps that need to be taken.
- Enforcement notice: The Commissioner may investigate any allegations of contravention of the PDPO and serve an enforcement notice on the data user prescribing, among other things, remedial action to be taken by the data user.
- Criminal liability: A data user who fails to comply with an enforcement notice commits an offense and is liable (a) on a first conviction to a fine at level 5 (currently HKD 50,000) and imprisonment for two years and, in the case of a continuing offense, to a daily penalty of HKD 1,000 and (b) on a second or subsequent conviction to a fine at level 6 (currently HKD 100,000) and imprisonment for two years and, in the case of a continuing offense, to a daily penalty of HKD 2,000. Further, a data user who, having complied with an enforcement notice, intentionally does the same act or makes the same omission in contravention of the requirement under the PDPO commits an offense and is liable on conviction to a fine at level 5 (currently HKD 50,000) and imprisonment for two years and, in the case of continuing offense, to a daily penalty of HKD 1,000.
- A person also commits an offense if the person (a) without lawful excuse obstructs, hinders or resists the Commissioner in performing its functions or exercising its powers, (b) without lawful excuse, fails to comply with any lawful requirement of the Commissioner, or (c) in the course of the performance or exercise by the Commissioner of functions or powers, (i) makes a statement to the Commissioner that the person knows to be false or does not believe to be true or (ii) otherwise knowingly misleads the Commissioner. A person who commits such offense is liable on conviction to a fine at level 3 (currently HKD 10,000) and imprisonment for six months.
- Civil liability: In addition to the above, any data subject who suffers damage (including injury to feelings) by reason of a contravention of any requirement under the PDPO (including the contravention of a DPP) by a data user may claim compensation from the data user for the damage.

8. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee’s personal data?

Employers should familiarize themselves with the DPPs. They should ensure that they have provided the PICS to relevant individuals before collecting such individuals’ personal data and that the various purposes for which personal data may be used by the employers is broad enough to cover the requirements of the employers.





 In Brief

 In Detail

Hong Kong

In Detail

An employer should be aware that an employee can access and obtain a copy of any of the employee’s personal data held by the employer (unless an exception applies) by serving a data access request (“**DAR**”) on the employer. DARs have become a favorite tactic of aggrieved employees looking to find a lever against their former employers. However, employers are becoming increasingly sophisticated in finding reasons to refuse to comply with such DARs. Therefore, a key issue for any employer is to minimize the creation of “personal data,” especially in a dispute or potential dispute. It is recommended that employers do not use employees’ names in emails and train business teams to speak to each other on sensitive issues rather than corresponding by email.

Contributed by: **Duncan Abate & Hong Tran**, Mayer Brown



[Link to biography >](#)



[Link to biography >](#)



HOME



COUNTRIES



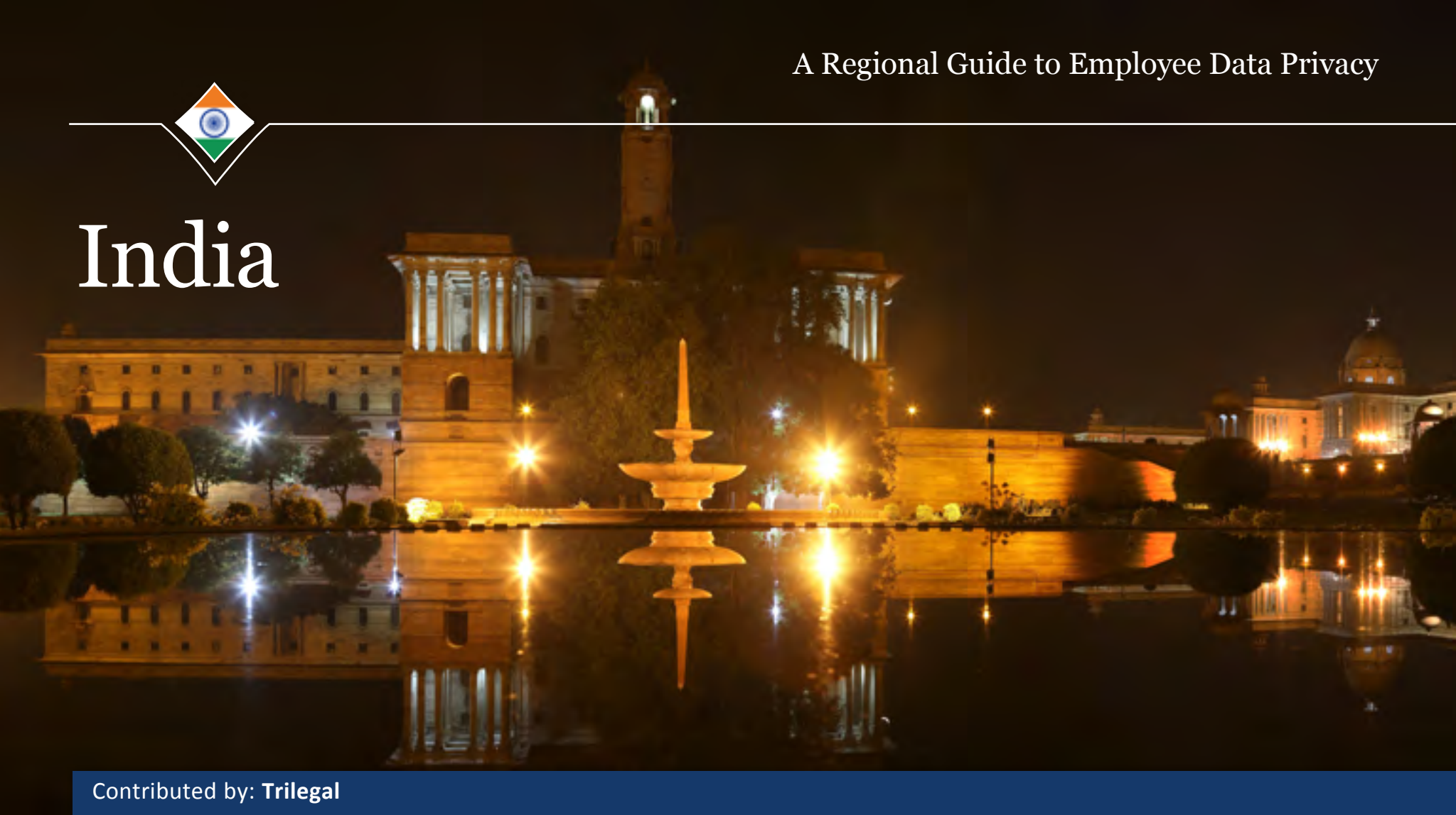
DIRECTORY

August 2018

SCROLL DOWN 



India



Contributed by: **Trilegal**



In Brief



In Detail

Contributed by: **Ajay Raghavan & Swarnima**, Trilegal



[Link to biography >](#)



[Link to biography >](#)



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



India

In Brief

1. Is there a law regulating applicant personal data?

While there is no law that specifically regulates only personal data, in general, the collection, use, transfer and storage of personal data containing personal information (“PI”) and sensitive personal information (“SPI”) is regulated by the Information Technology Act 2000 (“IT Act”) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (“Data Protection Rules”).

2. Is there a law regulating employee personal data?

Employee personal data are also regulated under the IT Act and Data Protection Rules. These laws apply to all “body corporates” (e.g., employers or companies) dealing with all forms of data in electronic form containing PI and/or SPI.

3. Do I need to have a privacy statement or agreement?

Employers collecting personal data are required to publish a privacy policy on their websites covering the stipulations under Rule 4 of the Data Protection Rules. Further, employers are required to obtain consent from the information provider (e.g., applicant or employee) prior to the collection of SPI and also to inform the applicant or employee of the purposes for which the information is being collected. No such consent is required before obtaining/collecting PI.

4. How long must I retain employee data? What is best practice?

There is no maximum statutory period prescribed for retaining general employee data. However, where the employee data contains SPI, such SPI cannot be retained for longer than it (a) is required under law or (b) is required for the purpose for which the SPI may lawfully be

used. It should be noted that the IT Rules apply only to the collection and retention of PI/SPI in electronic form and do not apply to information stored in physical copies.

5. Can I transfer employee data overseas?

An employer is able to transfer SPI to any other company/ persons in other countries, but only if the receiving entity ensures the same level of data protection as is required under the Data Protection Rules. Further, SPI can only be transferred with the consent of the employee, unless such transfer is necessary for performing a lawful contract between the transferor and the employee. There are no specific requirements/restrictions associated with the transfer of PI overseas.

6. Can I transfer employee data to a third party?

The restrictions discussed in question 5 above will apply to the transfer of employee data to any other company/ person/third party, whether in India or overseas.

7. What are the consequences of breach?

If an employer is negligent in implementing and maintaining reasonable security practices as specified under the Data Protection Rules, resulting in a wrongful loss or wrongful gain to any person, then the employer would be liable to pay compensation to the person so affected. In relation to any other contravention of the Data Protection Rules, the employer would be liable to pay compensation to the affected party or pay a penalty.

8. What are the main pitfalls?

Given that there have not been any reported judgments with respect to the enforcement of the provisions under the Data Protection Rules, the practical pitfalls with respect to enforcement actions under the Data Protection Rules have not yet presented themselves. However, a new data protection law is on the horizon.



India

In Detail

1. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant’s personal data in your jurisdiction?

Yes. India has specific rules that apply to companies dealing with personal information (“PI”) and sensitive personal information (“SPI”) under the Information Technology Act 2000 (“IT Act”) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (“Data Protection Rules”).

Under the Data Protection Rules, PI means “any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.” Further, SPI is defined as “any PI that contains information relating to passwords; financial information; physical, physiological and mental health condition; sexual orientation; medical history and records; and biometric information.”

The Data Protection Rules require employers to comply with certain obligations relating to collection, storage, retention, transfer and disclosure of SPI. In discharge of these obligations, companies often publish a detailed privacy policy on their websites (as discussed in response to question 3 below). Normally, when individuals make their job applications, companies require them to sign off on a consent letter to enable the companies to collect their SPI and conduct background checks. Some companies also obtain such consent in the offer letters issued to applicants who are shortlisted after the interview. Given the general practice in India is to issue offer letters prior to the date of joining (around one to three months in advance), companies typically use the gap between the time of making the offer and the date of joining to conduct background checks on the shortlisted applicants.

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee’s personal data in your jurisdiction?

Employee personal data are also regulated under the IT Act and Data Protection Rules. These laws apply to all employers dealing with all forms of data in the electronic form containing PI and/or SPI.

3. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee’s personal data?

Yes. All employers dealing with PI and SPI under the IT Act and Data Protection Rules must publish a privacy policy on their websites providing for (a) practices and policies with regard to data use and protection, (b) the types of PI and SPI





India

In Detail

being collected, (c) the purpose of collection and usage of information, (d) details regarding the disclosure of information and (e) the implementation of reasonable security practices and procedures. The policy must also be made available to the employee.

Further, employers are required to obtain consent from the employee prior to the collection of SPI. The employers would have to ensure that SPI is collected for a lawful purpose and that the collection of such SPI is necessary for that purpose. Further, employers would need to give the employee an option to not provide her/his data. If such person agrees to provide her/his data containing SPI, then the employer would need to obtain her/his written consent (or consent through fax, by email or electronic communication). While collecting SPI from the employee, the employer should inform such person of:

- the fact that SPI is being collected;
- the purpose for which the SPI is collected;
- the intended recipients of the SPI; and
- the names and addresses of the agencies that would collect and retain the SPI.

No such consent is required before obtaining/collecting PI from applicants or employees.

4. For how long must an employer retain an employee's personal data? What is best practice?

There is no maximum period for which an employee's personal data can be retained. The IT Act and the Data Protection Rules only clarify that the SPI and PI in their electronic form cannot be retained for longer than it (a) is required under law, or (b) is required for the purpose for which the SPI may lawfully be used. An employer should retain employee personal data for at least three years, as the laws on limitation provide that civil legal proceedings may be initiated during such period. The Indian Income Tax Act 1961 provides that the Income Tax department may initiate proceedings against a person during any of the seven assessment years succeeding the relevant assessment year. Companies therefore usually retain financial information, including that relating to employees, for a minimum period of eight years.





India

In Detail

5. What are the legal restrictions on transferring employees' personal data outside your jurisdiction?

An employer is able to transfer SPI to any other company/person in other countries, only if the receiving entity ensures the same level of data protection as is required under the Data Protection Rules. For instance, one such level of data protection is the company's requirement to maintain reasonable security practices and standards, such as implementing the security standard - IS/ISO/IEC 27001 "Information Technology–Security Techniques–Information Security Management System Requirements."

Further, SPI can only be transferred with the consent of the employee, unless such transfer is necessary for performing a lawful contract between the transferor and the employee. There are no such restrictions on the transfer of PI outside the country.

6. What are the legal restrictions on transferring employees' personal data to a third party?

The restrictions discussed in question 5 above will apply to the transfer of employee data to any other company/person/third party, whether in India or overseas.

7. What are the consequences of breaching privacy laws in your jurisdiction?

Since there are no specific laws pertaining to data privacy in India, civil action may be initiated under tort law. Separately, with respect to data privacy breaches, if the employer is negligent in implementing and maintaining reasonable security practices as specified under the Data Protection Rules, resulting in a wrongful loss or gain to any person, then the employer would be liable to pay compensation to the person so affected. In relation to contravention of any other obligation under the Data Protection Rules, employers can be required to pay compensation of up to INR 25,000 (approximately USD 350) to the persons affected by such noncompliance or to pay a penalty of up to INR 25,000 (approximately USD 350).

8. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee's personal data?

Given that there have not been any reported judgments with respect to the enforcement of the provisions under the Data Protection Rules, the practical pitfalls with respect to enforcement actions under the Data Protection Rules have not yet presented themselves.





India

In Detail

It is important to note here that the government recently set up a Committee of Experts to identify key data protection issues in India and to draft dedicated data protection legislation. This Committee of Experts has submitted a draft of the Personal Data Protection Bill 2018 to the Ministry of Electronics and Information Technology. The Bill has now been published by the Ministry on its website to allow the public to provide their comments. This Bill remarks that the right to privacy is a fundamental right, and broadly seeks to provide a legal framework to protect the autonomy of individuals in relation to their personal data, set out the appropriate usage of personal data, create trustworthy relations between individuals and the entities processing their data, and specify the rights of such individuals. After scrutiny of the public comments, the Bill is likely to be introduced into Parliament for enactment. If enacted (perhaps in 2019), this law is likely to change the current legal position around data protection in India.

Contributed by: **Ajay Raghavan & Swarnima**, Trilegal



[Link to biography >](#)



[Link to biography >](#)



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Indonesia

Contributed by: **SSEK Indonesian Legal Consultants**



In Brief



In Detail

Contributed by: **Fahrul S. Yusuf**, SSEK Indonesian Legal Consultants



[Link to biography >](#)



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN

Indonesia

In Brief

1. Is there a law regulating applicant personal data?

There is no specific law regulating applicant personal data. Generally, the Human Rights Law provides the right to privacy, while the handling of digital personal data in Indonesia is specifically regulated under Minister of Communication and Informatics (“**MOCI**”) Regulation No. 20 of 2016 regarding the Protection of Personal Data in Electronic Systems (“**MOCI Reg 20**”).

2. Is there a law regulating employee personal data?

There is no specific law regulating employee personal data. Depending on the form of the employee personal data, MOCI Reg 20 and the Human Rights Law would generally be applicable.

3. Do I need to have a privacy statement or agreement?

If the employee’s personal data are electronically processed, then a written document stipulating the consent given by the employee to the employer to handle the personal data is required.

If the employee’s personal data are physical (i.e., not digitalized), then there is no legal requirement to have a document to deal with the employee’s personal data. However, it is recommended that employers include a statement detailing their right to use employee personal data in the Company Regulation (work rules).

4. How long must I retain employee data? What is best practice?

Data stored in an electronic system must be retained for at least five years unless otherwise regulated. The retention period for physical data that is not stored in an electronic system is at the discretion of the board of directors, with the best practice being at least two years after termination of employment.

5. Can I transfer employee data overseas?

Yes, subject to obtaining the employee’s consent and fulfilling the requirements under MOCI Reg 20 for electronic employee data.

6. Can I transfer employee data to a third party?

Yes, subject to obtaining the employee’s consent.

7. What are the consequences of breach?

Under MOCI Reg 20, the unauthorized handling of personal data or the handling of personal data that is not in accordance with MOCI Reg 20 may result in administrative sanctions. In theory, causes of action may also include civil tort, civil or criminal defamation, or criminal “unpleasant act”.

8. What are the main pitfalls?

Employee personal data should be handled responsibly and should not be abused in any way in order to avoid embarrassment or other damages being incurred by the employee, which may give rise to the above-mentioned causes of action.





Indonesia

In Detail

1. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant’s personal data in your jurisdiction?

There is no law or regulation that specifically regulates the collection, use and/or handling of an applicant’s personal data, including protection of the privacy of an applicant’s particulars. The Minister of Communication and Informatics (“**MOCI**”) relatively recently issued Regulation No. 20 of 2016 regarding the Protection of Personal Data in Electronic Systems (“**MOCI Reg 20**”), which stipulates the protections afforded to personal data stored in an electronic system. The MOCI Reg 20 acts as an implementing regulation of Law No. 11 of 2008 regarding Electronic Information and Transaction, last amended by Law No. 19 of 2016 (“**ITE Law**”), which requires the utilization of a person’s personal data through electronic media to be based on consent.

While there is no regulation that stipulates the protection of non-electronic personal data, generally, all persons have a general right to privacy under the Human Rights Law. Typically, employers or prospective employers would insert a clause regarding the use of the applicant’s or employee’s data in the application form (although this is not standard practice) or the employment agreement.

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee’s personal data in your jurisdiction?

Please refer to our response to question 1 above.

3. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee’s personal data?

If the employee’s personal data are handled electronically, then the personal data protection regime under MOCI Reg 20 will be applicable. Although not applicable as a framework for the protection of all personal data (i.e., it does not regulate the protection of non-electronic personal data), MOCI Reg 20 provides a solid foundation on previously undefined terminologies. For example, MOCI Reg 20 finally offers a definition of “personal data,” which is certain individual data that are stored, maintained, and preserved for its accuracy and protected of its confidentiality. “Electronic system” is defined as a series of electronic equipment and procedures that serve to prepare, collect, process, analyze, store, show, announce, deliver and/or distribute electronic information. Therefore, any personal data that is digitalized would fall under the ambit of MOCI Reg 20.





Indonesia

In Detail

MOCI Reg 20 requires any handling of electronic personal data to be done in accordance with the consent given by the personal data owner. This requirement is contained in Article 6 of MOCI Reg 20, which stipulates that an electronic system provider conducting certain processing of personal data (e.g., obtaining, collection, storage, destruction, etc.) must provide a consent form in the Indonesian language to obtain the consent of the personal data owner. There is no particular format provided by MOCI Reg 20 in respect of the consent form aside from the requirement that it be in writing. Therefore, if an employer wishes to handle an employee’s electronic personal data, it must first obtain the consent of the employee for such specific handling by obtaining a signed written consent form.

However, the law becomes less clear when the pertinent employee’s personal data are exclusively physical. In general, there is no legal requirement to have a document to deal with such employee’s physical personal data. Nonetheless, we would recommend that the employer include a statement detailing its rights in respect of the use of employee personal data in the Company Regulation (work rules) that is binding on all employees to cover all bases.

4. For how long must an employer retain an employee’s personal data? What is best practice?

Manpower laws and regulations do not expressly deal with employee data privacy. In light of this, reference can be made to MOCI Reg 20, as well as Law No. 8 of 1997, regarding Corporate Documents (“**Law No. 8**”).

First, Article 15 paragraph (3) of MOCI Reg 20 requires personal data stored in electronic systems to be stored for at least five years unless otherwise regulated. The five-year period commences on the date a party ceases to be a user of an electronic system. After the five-year period has elapsed, the personal data may be erased unless such data are still being used or utilized in line with the initial purpose for which they were obtained and collected.

Separately, to the extent that the employee’s personal data are not encrypted in an electronic system, reference shall be made to Law No. 8 as the primary regulation on maintaining corporate documents. Articles 3 and 4 of Law No. 8 differentiate between (i) financial documents and (ii) other documents. Financial documents consist of records, bookkeeping documentation and financial administration supporting data, that evidence the rights, obligations, financial affairs and business activities of a company. “Other documents” consist of data or any writings containing information having effective value for a company even though not directly related to financial documents.

The Elucidation of Article 4 of Law No. 8 mentions that other documents include minutes of general meetings of shareholders, a company’s deed of establishment, other authentic deeds containing specific legal interests and a company’s taxpayer registration number. “Employee personal data” is not expressly mentioned as an example of





Indonesia

In Detail

“other documents” in the Elucidation. However, it is prudent to treat employee personal data as “other documents” and to apply the related rules as follows.

Pursuant to Article 11 paragraph (3) of Law No. 8, the retention term of other documents (i.e., employee files) shall be based on the usage value of such documents. The term shall be determined at the discretion of the board of directors.

Pursuant to Article 96 of Law No. 13 of 2003 regarding Manpower, there is a two-year limitation period for employee claims. We therefore recommend that physical, non-encrypted employee personal data be retained for at least two years after termination of employment.

5. What are the legal restrictions on transferring employees’ personal data outside your jurisdiction?

Under Article 22 of MOCI Reg 20, a party domiciled in Indonesia that wishes to effect the offshore transfer of personal data must coordinate with the MOCI or an authorized official/institution, which encompasses (i) reporting the planned data transfer, including at least information on the receiving state, the receiver, the date of transfer, and the purpose of such offshore transfer; (ii) requesting advocacy, if necessary; and (iii) reporting the result of the data transfer. It must also implement the regulatory provisions on offshore data transfers.

It should be noted that, as at the date of writing, the enforcement of these requirements is unclear. No implementing regulations have been issued to clarify the requirements on coordination with the MOCI, nor is there any existing regulation that specifically regulates offshore data transfers. Under existing regulations, the only applicable regulatory provision for offshore data transfers—or any data transfer, in fact—would be the general requirement to obtain the consent of the data owner for such offshore data transfer.

Notwithstanding the above, we recommend that the employer’s right to perform offshore data transfers be clearly stipulated in the Company Regulation.

6. What are the legal restrictions on transferring employees’ personal data to a third party?

There is no legal restriction on transferring an employee’s personal data to a third party as long as the consent of the employee is obtained by the employer. We recommend that the employer’s right to transfer employee personal data to a third party be stipulated in the Company Regulation.





Indonesia

In Detail

7. What are the consequences of breaching privacy laws in your jurisdiction?

Article 36 paragraph (1) of MOCI Reg 20 stipulates that anyone who takes any action involving personal data without the appropriate permission or that is not in accordance with the provisions of MOCI Reg 20 or any other regulation shall be subject to administrative sanctions in the form of (a) verbal warning, (b) written warning, (c) temporary suspension of activities, and/or (d) publication of their name online.

Article 36 paragraph (2) of MOCI Reg 20 states that the implementation of the above sanctions shall be regulated in a separate MOCI regulation, which has not been issued as at the date of writing. Therefore, in practice, the enforcement of these sanctions is not strict.

Additionally, ITE Law imposes criminal sanctions for certain specified actions, such as unauthorized accessing, interception and wire-tapping, ranging from the imposition of a penalty to imprisonment.

Other than the above administrative sanctions, in theory, causes of action may include civil tort, civil or criminal defamation, or criminal “unpleasant act”. However, we are not aware of any such actions being taken in practice.

8. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee’s personal data?

Employee personal data should be handled responsibly and should not be abused in any way in order to avoid embarrassment or other damages being incurred by an employee, which may give rise to the above-mentioned causes of action.

Contributed by: **Fahrul S. Yusuf**, SSEK Indonesian Legal Consultants



[Link to biography >](#)



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Japan



Contributed by: **Anderson Mori & Tomotsune**

 In Brief

 In Detail

Contributed by: **Nobuhito Sawasaki**, Anderson Mori & Tomotsune

 [Link to biography >](#)



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Japan

In Brief

1. Is there a law regulating applicant personal data?

Yes. The Personal Information Protection Act (“PIPA”), the Employment Security Act (“ESA”) and the relevant guidelines regulate applicants’ personal data.

2. Is there a law regulating employee personal data?

Yes. The PIPA and the relevant guidelines regulate employees’ personal data.

3. Do I need to have a privacy statement or agreement?

Generally, no. However, in practice, it is quite common to establish a privacy policy as this is the most convenient way to satisfy an employer’s obligation regarding notice requirements, such as notification of the relevant purposes for the use of collected personal information.

4. How long must I retain employee data? What is best practice?

Certain important documents should be retained for two to five years.

5. Can I transfer employee data overseas?

Yes, so long as the transfer occurs within the same legal entity, no restrictions exist in transferring personal data overseas.

However, in principle, the transfer of personal data to a third party outside Japan (including an overseas parent or related company) requires the prior consent of the relevant employee.

6. Can I transfer employee data to a third party?

The relevant employee’s prior consent is required to transfer his/her personal data to a third party (including his/her employer’s group companies) unless an exemption under the PIPA applies.

7. What are the consequences of breach?

Fraudulent provision or use of a personal information database may lead to imprisonment of up to one year or a fine of up to JPY 500,000.

The relevant data privacy authority may issue a recommendation and/or an order to rectify the breach. Failure to comply with the order may lead to imprisonment of up to six months or a fine of up to JPY 300,000.

If a breach causes any damage, the person responsible for such breach and his/her employer may be liable for the damages.

8. What are the main pitfalls?

Special regulations exist for health-related information and other sensitive information.

When conducting background checks separately, it is necessary to obtain the job applicant’s consent for not only the collection of his/her sensitive data, but also the acquisition of personal data from third parties such as his/her former employers.





Japan

In Detail

1. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant’s personal data in your jurisdiction?

Yes. The main sources of obligations with respect to the protection of applicants’ personal data are the Personal Information Protection Act (Act No. 57 of 2003, as amended) (“**PIPA**”), the Employment Security Act (Act No. 141 of 1947, as amended) (“**ESA**”) and the various guidelines issued by government agencies. In particular, the guidelines issued by the Personal Information Protection Commission (“**PIPC**”) (the “**PIPC Guidelines**”) and the ESA guidelines issued by the Ministry of Health, Labor and Welfare (“**MHLW**”) (the “**ESA Guidelines**”) are most relevant to the handling of applicants’ personal data.

If an employer intends to conduct a background check on a job applicant, the employer must obtain the applicant’s consent before the acquisition of personal data from third parties (such as his/her former employers), because, in principle, third parties are prohibited from providing a job applicant’s personal data without his/her consent while the employer is permitted to collect such information without consent (other than the exceptions outlined below).

In addition, under the PIPA, the MHLW Health Data Guidelines and the ESA Guidelines, if an employer wishes to collect certain sensitive information from a job applicant, in principle, the employer must obtain the applicant’s prior consent.

Further, if an applicant’s personal data are shared among group companies (including those located outside Japan), in principle, the employer must obtain the applicant’s consent before the personal data are shared.

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee’s personal data in your jurisdiction?

Yes. The main sources of obligations with respect to the protection of employees’ personal data are the PIPA and the various guidelines issued by government agencies. In particular, the PIPC Guidelines and the guidelines concerning employees’ health data issued by the MHLW (the “**MHLW Health Data Guidelines**”) are most relevant to the handling of employees’ personal data.





Japan

In Detail

3. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee’s personal data?

Generally, no. There is no provision in the PIPA or the ESA that expressly requires a privacy statement or agreement.

However, under the PIPA, upon obtaining the personal data of an employee, an employer must promptly either (i) publicly announce the relevant purposes of use of the personal data; or (ii) individually notify the relevant employee of the relevant purposes of use of the personal data (unless such purposes of use have previously been publicly announced). In addition, if employees’ personal data are retained for longer than six months, the employer must notify such employees of certain matters, such as its name registered on the commercial registry, procedures for a request of disclosure and correction of their own personal data.

So, in practice, it is quite common to establish a privacy policy and post it on an intranet as this is the most convenient way to satisfy the employer’s above obligation.

4. For how long must an employer retain an employee’s personal data? What is best practice?

An employer is required to retain certain important documents for a statutory period. For example, under the Labor Standards Act (“LSA”), an employer is required to retain the workers’ register, payroll book, and other important documents relating to hiring, dismissal, occupational accidents, wages and other matters relating to employment for three years from the date designated by the LSA. In addition, an employer must keep documents regarding health insurance, employees’ pension insurance, workers’ accident compensation insurance, unemployment insurance and other statutory insurance that the employer is obliged to prepare by the relevant law, for each statutory period (two years to five years).

Separately, under the PIPA, if employees’ personal data are no longer needed in light of the relevant purposes of use, the data should be destroyed or deleted without delay. Accordingly, except for basic and important information required to be retained by the relevant law, an employer should destroy or delete an employee’s personal data as soon as possible when they are no longer needed.





Japan

In Detail

5. What are the legal restrictions on transferring employees' personal data outside your jurisdiction?

No particular restrictions exist when an employer transfers employees' personal data outside Japan so long as the transfer occurs within the same legal entity (i.e., to an overseas office of the same company).

However, when an employer transfers employees' personal data to a third party outside Japan (including its group companies outside Japan), the employer must obtain the employee's prior consent unless:

- (a) the receiving third party is in any of the countries specified by the PIPC as having personal information protection systems that are at least as stringent as those in Japan; or
- (b) the receiving third party has put in place personal information protection systems that meet the standards specified by the PIPC.

As for (a), as at the date of writing, the EU will be recognized by the PIPC this fall as having personal information protection systems that are at least as stringent as those in Japan. As for (b), it is common to execute a data transfer agreement between the parties.

Even if one of the exceptions above applies, an employer must comply with third-party transfer regulations as explained in question 6 below.

6. What are the legal restrictions on transferring employees' personal data to a third party?

The relevant employee's prior consent is required to transfer his/her personal data to a third party (including the employer's group companies) unless an exemption under the PIPA applies.

There are several types of exemptions. The first type of exemption is where it is legally required or where it is necessary to protect the life, body or asset of a person and it is difficult to obtain the relevant employee's consent.

Another type of exemption involves outsourcing agents and a so-called Specified Sharing Scheme. If an employer outsources the processing of the personal data of its employees, to the extent it is necessary to perform the services outsourced to the agent, the outsourcing agent is not regarded as a third party. If a Specified Sharing Scheme is used, the parties participating in such Specified Sharing Scheme are not regarded as third parties either. In both cases, the employer is not required to obtain the relevant employee's prior consent.





Japan

In Detail

7. What are the consequences of breaching privacy laws in your jurisdiction?

If an officer, an employee, a former officer or a former employee has provided or fraudulently used a personal information database that they had been handling in relation to their business for the purpose of seeking their own or a third party's illegal profits, such person is subject to imprisonment for up to one year or a fine of up to JPY 500,000. In addition, the legal entity to which such person belongs may be subject to a fine of up to JPY 500,000.

When there is a breach of the PIPA, the relevant data privacy authority may issue a recommendation to rectify the breach. If a person fails to comply with the recommendation without due cause, the relevant data privacy authority may issue an order to comply with it. If the person fails to comply with the order, the person is subject to imprisonment for up to six months or a fine of up to JPY 300,000. In addition, the legal entity to which such person belongs may be subject to a fine of up to JPY 300,000.

If a breach causes any damage, the person responsible for such breach and his/her employer may be liable for the damages as a result thereof.

8. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee's personal data?

Under the PIPA, if an employer obtains certain sensitive information such as race, creed, social status, medical history and/or criminal history, in principle, the employer must obtain prior consent from the relevant applicant and/or employee before collecting, using and/or handling this data.

The MHLW Health Data Guidelines and the ESA Guidelines also provide special regulations regarding the collection, use and handling of health-related information and other sensitive information of employees and applicants.

When an employer conducts background checks on job applicants, it is necessary to obtain consent from the job applicants (ideally in writing) not only for the collection of their sensitive data, but also for the acquisition of personal data from third parties such as his/her former employers because, as explained above, in principle, third parties are prohibited from providing former employees' personal data without their consent.

Contributed by: **Nobuhito Sawasaki**, Anderson Mori & Tomotsune



[Link to biography >](#)



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Macau



Contributed by: **MdME Lawyers**



In Brief



In Detail

Contributed by: **Tiago Vilhena & António Tam**, MdME Lawyers



[Link to biography >](#)



[Link to biography >](#)



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



Macau

In Brief

1. Is there a law regulating applicant personal data?

Yes. Personal data in Macau is regulated by Law No. 8/2005 (the “**Data Protection Law**” or “**MDPL**”). MDPL regulates the legal regime for collecting, processing and transferring personal data and applies generally to everyone, including applicants.

2. Is there a law regulating employee personal data?

Yes. Besides the general protection granted by MDPL, there are legal provisions in the Macau Labor Relations Law and in scattered authorizations and guidelines from the Macau Data Protection Office addressing employee personal data issues.

3. Do I need to have a privacy statement or agreement?

Privacy statements or agreements are not compulsory. It is recommended, however, that employers have a Personal Information Collection Statement executed by employees.

4. How long must I retain employee data? What is best practice?

Employment legislation requires an employer to retain employee data during the whole duration of the employment relationship and for a period of three years after its termination. This is subject to the limitation period for potential claims.

5. Can I transfer employee data overseas?

Yes, subject to certain requirements.

6. Can I transfer employee data to a third party?

Yes, subject to certain requirements.

7. What are the consequences of breach?

The legal consequences of a breach range from monetary fines to imprisonment and accessory sanctions.

8. What are the main pitfalls?

The main pitfalls are generally associated with the failure to obtain an unambiguous consent from employees when processing their personal data and the failure to comply with the notifications and prior authorization requirements set forth in the MDPL.





Macau

In Detail

1. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant's personal data in your jurisdiction?

Data protection in Macau is regulated by Law No. 8/2005 (the “**Data Protection Law**” or “**MDPL**”), which establishes the legal regime for collecting, processing and transferring personal data. This applies generally to everyone, including applicants.

For the purposes of MDPL, “personal data” is defined as “*any information of any type, irrespective of the type of medium involved, including sound and image, relating to an identified or identifiable natural person*” (Article 4 No. 1), whereas the concept of “processing of personal data” is defined as “*any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction*” (Article 4 No. 3).

The public regulatory entity charged with monitoring and enforcing the compliance with the provisions of the Data Protection Law is the Macau Data Protection Office, created under the Chief Executive’s Dispatch No. 83/2007 (the “**MDPO**”).

Besides MDPL, which establishes the general framework for personal data collection and treatment, MDPO has issued the Authorization No. 01/2011, under which employers are exempted from notifying the MDPO when processing certain data relating to job applicants, such as name, place of birth, gender, résumé information, etc., under and for the purposes of a recruitment procedure.

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee's personal data in your jurisdiction?

Apart from the generic provisions set out in the MDPL, Law No. 7/2008 (“**Labor Relations Law**” or “**MLRL**”) establishes specific rules regarding the collection and keeping of employee personal data.

Under Article 13 of the MLRL, the employer is obliged to keep, for a period of not less than three years after termination of the employment relationship, the records of employee data, which should include:

- (a) personal data of the employee, including his/her name, sex, age and form of contact;





Macao

In Detail

- (b) the date of admission;
- (c) the professional grade or function;
- (d) detailed pay slips;
- (e) the normal working hours;
- (f) the holidays taken;
- (g) the total number of days' absence and the number of days' paid sick leave or accident leave;
- (h) occupational accidents and diseases; and
- (i) all data provided by the employee that contribute to the protection of his/her interest.

Violation of any of the above obligations is considered to be an administrative misdemeanor, punishable with a fine, ranging from MOP 1,000 to MOP 5,000 for each employee involved.

Further to the above, MDPO has also issued a detailed Guideline in respect of employee monitoring in the workplace. Under this Guideline, prior to conducting employee monitoring, the employer must formulate Personal Information Collection Statements (“**PICS**”), which clearly address the following points:

- (a) The purpose of employee monitoring;
- (b) The categories of the personal data to be collected for monitoring;
- (c) The uses of the personal data collected for monitoring, which should not deviate from the purpose of monitoring;
- (d) The criteria for using the personal data collected for monitoring;
- (e) Authorized personnel with access to the data processed from monitoring, such as the personnel operating and monitoring the video and recording facilities, and the personnel with the right of access to the relevant data;





Macao

In Detail

- (f) Generally, the duration of the data processed for monitoring should not exceed six months, unless the law or contract terms stipulate a longer duration or the relevant records have become evidence of disciplinary, administrative or criminal infringement;
- (g) The employees’ right to information, right of access and to rectify data, and right to object should be clearly stated, as should the regulations on the reasonable fees charged for the employees to exercise their right of access and right to consult data. The fees charged are on a case-by-case basis but the employees concerned should be informed of the fees before exercising this right; and
- (h) The formulation of “house rules” regarding employees using the institution’s facilities for private or personal use.

3. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee’s personal data?

Under Article 6 of the MDPL, the collection and treatment of personal data are only admissible if the relevant data subject provides his/her unambiguous consent to the said treatment or if the processing of personal data is required:

- (a) for the performance of a contract or contracts to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract or a declaration of his/her will to negotiate;
- (b) for compliance with a legal obligation to which the controller is subject;
- (c) in order to protect the vital interests of the data subject if he/she is physically or legally incapable of giving his/her consent;
- (d) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
- (e) for pursuing the legitimate interests of the controller or the third party to whom the data are disclosed, except where such interests should be overridden by the interests for fundamental rights, freedoms and guarantees of the data subject.





Macau

In Detail

Article 10 of the MDPL sets out the Right to Information of the data subject, which must be ensured by the entity collecting and treating personal data in Macau, under which the holders of personal data are entitled to receive information regarding the data they provide, namely:

- (a) The identity of the entity collecting and treating the data and of its representative in Macau, if necessary;
- (b) The purposes of the processing;
- (c) Other information such as:
 - (i) The recipients or categories of recipients of the data;
 - (ii) Whether replies are obligatory or voluntary, as well as the possible consequences of failure to reply; and
 - (iii) The existence and conditions of the right of access and rectification.

The information to be provided must be set out in the documents supporting the collection of data (e.g., on the website).

Therefore, although it is not compulsory to enter into a privacy statement with employees, it is recommended that employers have a PICS executed by the employees to guarantee that the employees' Right to Information is duly complied with and their unambiguous consent has been duly obtained.

4. For how long must an employer retain an employee's personal data? What is best practice?

MLRL requires employers to keep records of employee data, with the information listed in question 2, throughout the entire duration of the employment relationship, and for a period of not less than three years after it terminates.

However, from a litigation perspective, the statutory limitation period for credits resulting from labor relations (e.g., salaries, commissions, subsidies, overtime payments, etc.) is 15 years under the Macau Civil Code. This period runs from two years after the termination of the employment relationship. For full protection against future claims, therefore, it is best practice for employers to keep employee data for 17 years after termination of employment.





Macau

In Detail

5. What are the legal restrictions on transferring employees' personal data outside your jurisdiction?

According to Article 19 of the MDPL, the transfer abroad of data collected in Macau is subject to authorization by the MDPO, upon verification of whether the target jurisdiction to which the data is transmitted affords an adequate level of protection.

Despite the above, Article 20 of the MDPL sets out certain exceptions to this requirement of prior authorization, by allowing the transfer, *inter alia*, (a) in the case of unambiguous consent by the data holder; (b) when the transfer of data is necessary for the performance of a contract between the data holder and the entity collecting and treating the data; (c) when the transfer of data is necessary for the performance or execution of a contract executed or to be executed, in the interest of the data subject, between the controller and a third party; or (d) when the transfer of data is necessary or legally required on important public interest grounds, or for the establishment and exercise of defense of legal claims.

In these cases, set out in Article 20, number 1, paragraphs (1) to (5) of the MDPL, the notification to the MDPO shall suffice for the purposes of validly effecting a transfer of data to a jurisdiction outside of Macau.

6. What are the legal restrictions on transferring employees' personal data to a third party?

Unambiguous consent must be obtained before transferring employees' personal data to any third parties within the territory of Macau.

However, the transfer of data, as one of the ways to process data, must be:

- (a) processed lawfully and with respect for the principle of good faith and the general principle, under which the processing of personal data shall be carried out transparently and with strict respect for privacy and for other fundamental rights, freedoms and guarantees set out in the Basic Law of Macau, the instruments of international law and the legislation in force;
- (b) carried out for specified, explicit, legitimate purposes and for purposes directly related to the activity of the employer and not further processed in a way incompatible with those purposes;
- (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;





Macau

In Detail

- (d) accurate and, where necessary, kept up to date (adequate measures must be taken to ensure that data that are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified); and
- (e) kept in a form that permits identification of their subjects for no longer than is necessary for the purposes for which they were collected or for which they are further processed.

7. What are the consequences of breaching privacy laws in your jurisdiction?

The MDPL sets out in Articles 30 to 43 the applicable administrative and criminal sanctions applicable to infractions of the MDPL.

From an administrative perspective, these infractions may entail fines ranging from MOP 2,000 to MOP 200,000, depending on the nature of the infractions.

Moreover, conduct such as intentionally omitting the statutory requests for notification and/or authorization set out in Articles 21 and 22 of the MDPL may result in prison sentences of up to two years or a fine of up to 240 days, up to the amount of MOP 2,400,000 (one day is defined under Macau law as an amount ranging between MOP 50 and MOP 10,000, to be determined by the court depending on the infringing party's financial status and capability). From a practical perspective, it is highly unlikely that prison sentences would be applied for these infractions, and, if so, it is likely that suspended sentences would be applied.

Moreover, Article 43 sets out additional penalties such as (a) temporary prohibition of collection of treatment of personal data; (b) an order to partially or fully erase the unduly collected data; (c) publication of the judgment against the infringing entity in the Macau newspapers and/or (d) public warning or censure of the infringing entity.

Violation of the employer's obligation under the MLRL to retain employee personal data (please see question 2) may also give rise to a fine, ranging from MOP 1,000 to MOP 5,000 for each employee involved.

8. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee's personal data?

Due to the increase in complaints associated with the mishandling of personal data and issues such as the regularity of collection of video footage by CCTV, there has been increased activity from the MDPO in respect of inspection and





Macau

In Detail

compliance actions with companies that collect, treat and transfer personal data in Macau, as well as an increase in the number of fines and sanctions applied to local entities for failure to comply with local provisions on data protection, particularly with respect to failure to communicate to the regulator the treatment and/or transfer of personal data in Macau.

As a general rule, the collection, treatment and transfer of personal data are subject to the issuance of a notice to the MDPO whereby the entity proposing to carry out these activities declares its intention to collect, treat and/or transfer personal data, within eight days after the commencement of treatment of personal data.

Moreover, notification requirements extend to the collection of all data, and not just data collected by means of CCTV, with specific provisions and requirements for collection and treatment of data of (a) employees (which may entail further requirements if the employer collects data such as health data for insurance coverage purposes); and (b) clients. As such, companies should have notifications in place for the collection, treatment and transfer of all of its data in Macau – or at least the data that are not covered by exemptions established by the MDPO – to minimize the risk of fines and potential criminal liability.

Contributed by: **Tiago Vilhena & António Tam**, MdME Lawyers



[Link to biography >](#)



[Link to biography >](#)



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Malaysia



Contributed by: **Shearn Delamore & Co.**



In Brief



In Detail

Contributed by: **Wong Kian Jun**, Shearn Delamore & Co.



[Link to biography >](#)



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Malaysia

In Brief

1. Is there a law regulating applicant personal data?

Yes, the Personal Data Protection Act 2010 (“PDPA”).

2. Is there a law regulating employee personal data?

Yes, the PDPA.

3. Do I need to have a privacy statement or agreement?

Yes, this is required under the PDPA.

4. How long must I retain employee data? What is best practice?

The Employment Act 1955 provides that a register containing information relating to an employee must be kept and be available for inspection for not less than six years after recording.

The PDPA, however, only provides that the personal data should not be kept longer than necessary.

5. Can I transfer employee data overseas?

Generally speaking, no. However, there are certain exceptions that may apply to allow the transfer of employee data overseas.

6. Can I transfer employee data to a third party?

You can only transfer employee data to a third party if you have obtained the consent of the employee.

7. What are the consequences of breach?

A breach of the provisions of the PDPA leads to a fine or a term of imprisonment or both. The sum of the fine or term of the imprisonment will vary depending on the type of breach.

8. What are the main pitfalls?

The ambiguity of the language in the PDPA may result in uncertainty over the application or interpretation of the principles under the PDPA.





Malaysia

In Detail

1. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant's personal data in your jurisdiction?

Yes, collecting and/or handling applicant data are regulated under the Personal Data Protection Act 2010 (“**PDPA**”), which came into force in 2013.

The PDPA provides, among other things, that the employer must comply with the seven Personal Data Protection Principles when managing applicant personal data:

(a) The General Principle

Under this principle, consent would be required to process the applicant's data.

(b) The Notice and Choice Principle

This principle requires a written notice to be issued to the data subject. Please see question 3 below.

(c) The Disclosure Principle

This principle governs the extent to which the personal data can be disclosed to other parties.

(d) The Security Principle

Under this principle, the data user (i.e., the employer) should take practical steps to protect the personal data.

(e) The Retention Principle

The personal data of the applicant shall not be kept longer than necessary for the fulfillment of the purpose for which they were collected.

(f) The Data Integrity Principle

The data user shall take reasonable steps to ensure that the personal data it retains relating to the applicant are accurate, complete, not misleading and kept up to date.





Malaysia

In Detail

(g) The Access Principle

The applicant shall be given access to his/her personal data held by a data user and be able to correct his/her personal data where the personal data are inaccurate, incomplete, misleading or not up to date.

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee’s personal data in your jurisdiction?

Yes. The PDPA provides for the use of personal data within Malaysia. The PDPA only applies to “commercial transactions.”

Section 2 defines commercial transactions as “any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance, but does not include a credit reporting business carried out by a credit reporting agency under the Credit Reporting Agencies Act 2010.”

Although the PDPA does not specifically provide for employer-employee relationships, the Personal Data Protection Department, the authority in charge of matters pertaining to personal data, has since issued a Public Consultation Paper [No.3/2014], clarifying that the PDPA is applicable in respect of the personal data of employees.

The Employment Act 1955 (“**the Employment Act**”) also contains provisions relating to employee information for employees covered by this Act. It provides that an employer should maintain a register with certain information relating to employees regarding personal details, terms and conditions of employment and details of wages and allowances earned during each wage period. Such information should be kept in the office, in the relevant employee’s place of employment, and should be available for inspection by the relevant authorities and the employee.

The Employment Act generally covers, among other things, employees earning RM 2,000 and below a month, those engaged in manual labor irrespective of salary and those overseeing individuals engaged in manual labor irrespective of salary.





Malaysia

In Detail

3. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee's personal data?

Yes. Under the PDPA, one of the principles to which employers need to adhere is the Notice and Choice principle. The Notice and Choice Principle provides that a data user is required to issue a written notice to inform the employee of, among other things, the purpose for which the data are collected, recorded, held or stored and certain third parties who may have access to the personal information.

This written notice is to be provided in the Malaysian National Language and in English.

4. For how long must an employer retain an employee's personal data? What is best practice?

The Employment Act provides that a register containing information relating to an employee must be kept and be available for inspection for not less than six years after recording.

As for personal data under the PDPA, the Retention Principle requires that the personal data of an employee "shall not be kept longer than is necessary for the fulfillment of that purpose." The PDPA does not strictly provide for a timeline as to how long an employer must retain an employee's personal data.

5. What are the legal restrictions on transferring employees' personal data outside your jurisdiction?

Generally, employers are not allowed to transfer employee personal data outside of Malaysia. However, they may do so where such a place is specified by the Minister of Communications and Multimedia.

Notwithstanding the above, an employer may also transfer the personal data of an employee outside of Malaysia where the employee has expressly provided consent or where the transfer is necessary for the performance of the contract between the employer and employee.

6. What are the legal restrictions on transferring employees' personal data to a third party?

To transfer employees' personal data to a third party, the Disclosure Principle under the PDPA requires the employer to obtain consent from the employees.





Malaysia

In Detail

7. What are the consequences of breaching privacy laws in your jurisdiction?

The consequences of breaching privacy laws in Malaysia are generally a fine or imprisonment or both. The amount of the fine or term of imprisonment will depend on the breach.

A breach of the principles under the PDPA in processing, collecting, storing or disclosing the personal data of an employee shall carry a fine of up to MYR 300,000 or an imprisonment term of two years or both. Similar fines and/or imprisonment terms may arise in the event the employer unlawfully transfers the personal data of an employee outside of Malaysia.

Any unlawful collection of personal data shall render an employer liable to a fine of up to MYR 500,000 or to an imprisonment term of a maximum of three years or both.

8. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee's personal data?

There are degrees of ambiguity when it comes to the principles as provided under the PDPA. For example, the Security Principle requires an employer to take “*practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction*”. However, the PDPA does not set out how such “practical steps” may be effected and it is up to each organization to determine the same. This ambiguity sets a different bar for every organization.

Similarly, the Retention Principle requires each data user to not keep the data longer than is necessary for the fulfillment of that purpose. The PDPA does not set out a strict timeline and allows each organization to determine what is reasonable.

The ambiguity in the provisions of the PDPA may therefore lead to a degree of uncertainty.

Contributed by: **Wong Kian Jun**, Shearn Delamore & Co.



[Link to biography >](#)



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Myanmar



Contributed by: **Rajah & Tann NK Legal Myanmar Company Limited**



In Brief



In Detail

Contributed by: **Chester Toh & Lester Chua**, Rajah & Tann NK Legal Myanmar Company Limited



[Link to biography >](#)



[Link to biography >](#)



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



Myanmar

In Brief

1. Is there a law regulating applicant personal data?

There is no overarching legislation regulating applicant or employee personal data privacy in Myanmar. However, the Myanmar Constitution does provide general protection for the privacy of correspondence and other communications of a Myanmar citizen. The Electronic Transaction Law 2004 (“ETL”) and the Law Protecting the Privacy and Security of Citizens 2017 (“PPSCL”) also contain certain provisions that could be relevant to the collection, use and/or handling of applicant or employee personal data.

2. Is there a law regulating employee personal data?

Please see response to question 1 above.

3. Do I need to have a privacy statement or agreement?

An agreement with the person whose information is being collected is required for compliance with the ETL. No agreement is required for the collection of applicant or employee data under other statutes. However, having an agreement in place is recommended.

4. How long must I retain employee data? What is best practice?

There is no legal or regulatory requirement for retention of employee data. However, best practice would be to retain employee data for at least six years after termination of the employment contract.

5. Can I transfer employee data overseas?

There are no legal restrictions on the transfer of employee data overseas but prior consent may be required in practice.

6. Can I transfer employee data to a third party?

There are no general restrictions on transferring employee data to third parties. However, the ETL prohibits the distribution of certain information if it has been created or modified to be detrimental to the interest of or to lower the dignity of any organization or person.

7. What are the consequences of breach?

Violation of the ETL or the PPSCL can lead to imprisonment and/or fines. Unauthorized transfers of employee data may also amount to a breach of employment contract in the event that the employment contract has a confidentiality clause. However, there is currently no requirement for a confidentiality clause to be included in an employment contract.

8. What are the main pitfalls?

Although there is no overarching legislation regulating the collection, use and/or handling of applicant or employee personal data, employers should be aware that there is legislation that regulates the collection, use and/or handling of employee information in Myanmar.





Myanmar

In Detail

1. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant's personal data in your jurisdiction?

There is no overarching legislation in Myanmar that regulates applicant or employee personal data privacy in Myanmar. However, Article 357 of the Myanmar Constitution offers general protection for the privacy and security of home, property, correspondence and other communications of Myanmar citizens.

In addition, certain laws such as the Electronic Transaction Law 2004 (“**ETL**”) and the Law Protecting the Privacy and Security of Citizens 2017 (“**PPSCL**”) contain provisions that may be relevant to the collection, use and/or handling of an applicant's personal data:

- (i) Section 34(d) of the ETL prohibits the distribution of information created, modified or altered by electronic technology to be detrimental to the interest of or to lower the dignity of any organization or any person;
- (ii) Section 8(b) of the PPSCL prohibits surveillance, spying or investigation of a Myanmar citizen in a manner that could disturb his/her privacy and security or affect his/her dignity; and
- (iii) Section 8(c) of the PPSCL also prohibits the interception or disturbance of a person's communication with another person or communications equipment.

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee's personal data in your jurisdiction?

Please see response to question 1 above.

3. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee's personal data?

There is no legal requirement to have documentation that sets out the company's policy on an employee's privacy or the company's policy on the collection, storage and/or processing of employee information. However, we recommend that a clause to this effect be included in the employment agreement or in an employee handbook that is incorporated into the employment agreement.





Myanmar

In Detail

4. For how long must an employer retain an employee’s personal data? What is best practice?

There is no legal or regulatory requirement for retention of an employee’s personal data. However, as the relevant limitation period for an employee to bring a court action based on a written and registered employment contract is six years, best practice would be to retain an employee’s personal data for at least six years after termination of the employment contract.

5. What are the legal restrictions on transferring employees’ personal data outside your jurisdiction?

There are no legal restrictions on transferring employees’ personal data outside Myanmar. However, in practice, the Myanmar labor offices may require that prior consent be obtained from the employees before the transfer of their personal data outside Myanmar.

6. What are the legal restrictions on transferring employees’ personal data to a third party?

There are no general restrictions on transferring employee data to third parties. However, Section 34(d) of the ETL prohibits the distribution of information created, modified or altered by electronic technology to be detrimental to the interest of or to lower the dignity of any organization or any person.

Furthermore, if there is a confidentiality clause protecting an employee’s personal data in the relevant employment contract, transferring that employee’s personal data to a third party without his/her consent would constitute a breach of contract. There is currently no implied duty of confidentiality under Myanmar law.

7. What are the consequences of breaching privacy laws in your jurisdiction?

Violation of a prohibition contained in Section 34 of the ETL can lead to a maximum imprisonment term of five years and/or a fine.

Violation of a prohibition contained in Section 8 of the PPSCCL can lead to imprisonment for a term of between six months to three years and a fine of between MMK 300,000 and MMK 1,500,000.





Myanmar

In Detail

8. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee’s personal data?

Although there is no overarching legislation on the collection, use and/or handling of an employee’s personal data, employers should be aware that there is legislation that regulates the collection, use and/or handling of employee information in Myanmar (i.e., the Myanmar Constitution, the ETL and the PPSCCL). Given the lack of statutory instruments that regulate employee privacy in particular (other than the general protection accorded under the Myanmar Constitution), we recommend that employment agreements include provisions that permit the employer to collect, store, process and share an employee’s personal information.

Contributed by: **Chester Toh & Lester Chua**, Rajah & Tann NK Legal Myanmar Company Limited



[Link to biography >](#)



[Link to biography >](#)



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



New Zealand



Contributed by: **Simpson Grierson**



In Brief



In Detail

Contributed by: **Carl Blake**, Simpson Grierson



[Link to biography >](#)



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



New Zealand

In Brief

1. Is there a law regulating applicant personal data?

Yes, the Privacy Act 1993 (“Privacy Act”).

2. Is there a law regulating employee personal data?

Yes, the Privacy Act.

3. Do I need to have a privacy statement or agreement?

This is not required by the Privacy Act but is recommended as a matter of best practice.

4. How long must I retain employee data? What is best practice?

The Privacy Act does not require information to be held for any fixed period. The emphasis in the Act is on not holding information for longer than is necessary.

However, there are various other statutes governing the minimum periods for which certain information must be held (for example, tax records must be held for seven years, and wage records must be held for six years).

5. Can I transfer employee data overseas?

The Privacy Act does not contain specific restrictions on the transfer of personal information overseas.

Individuals must be made aware of all intended recipients of their personal information at the time it is collected. If such notice is not provided, then the consent of employees must generally be obtained before transferring information to any other jurisdiction.

6. Can I transfer employee data to a third party?

The Privacy Act does not contain specific restrictions on the transfer of personal information to third parties.

Individuals must be made aware of all intended recipients of their personal information at the time it is collected. If such notice is not provided, then the consent of employees must generally be obtained before transferring information to any other entity/third party.

7. What are the consequences of breach?

- Investigation by the Privacy Commissioner (who can issue non-binding recommendations and publicly name an agency that is found to have breached the Privacy Act).
- Human Rights Review Tribunal (potential remedies include damages up to NZD 350,000).
- Administrative Penalties (may be liable on summary conviction for a fine not exceeding NZD 2,000).

Note that, under the recently introduced Privacy Bill 2018, changes are likely in this area.

8. What are the main pitfalls?

Common pitfalls include:

- The failure to properly notify an individual about the collection of personal information (in accordance with Information Privacy Principle (“IPP”) 3).
- The use of personal information for a purpose other than that for which it was obtained (prohibited by IPP 10).
- Improper disclosure of personal information (prohibited by IPP 11).





New Zealand

In Detail

1. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant’s personal data in your jurisdiction?

The Privacy Act 1993 (“**Privacy Act**”) regulates the collection, use and/or handling of an applicant’s personal information. Employers must comply with the Information Privacy Principles (“**IPP**”) set out in the Privacy Act during the recruitment process. The IPPs guide the collection, use, storage and disposal of personal information.

During the recruitment process, employers should ensure that:

- they only ask for personal information necessary to determine an applicant’s suitability for the role;
- the applicant is aware that the information is being collected, the purpose for which it is being collected, the intended recipients of the information, the consequences if all or any part of the requested information is not provided, and his/her rights of access to, and correction of, personal information provided;
- all reference checks are made with the applicant’s consent; and
- once the personal information collected has been used to assess the applicant’s suitability for the position, it is destroyed and not disclosed to others.

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee’s personal data in your jurisdiction?

Yes, the Privacy Act.

3. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee’s personal data?

The Privacy Act does not require employers to implement a privacy policy. However, an employer must ensure that one or more individuals are responsible for:

- encouraging and ensuring compliance with the Privacy Act;
- handling Privacy Act requests; and





New Zealand

In Detail

- working with the Privacy Commissioner in relation to investigations of the employer.

Further, an employer must (at the time the information is collected or, if that is not practicable, as soon as practicable after the information is collected) make an employee aware of:

- the fact that information is collected;
- the purpose for which the information is collected;
- the intended recipients of the information;
- the name and address of the agency that is collecting the information;
- the name and address of the agency that will hold the information;
- whether or not the collection of the information is authorized or required by law;
- the consequences to the data subject if the requested information is not provided; and
- the rights of access to, and correction of, personal information as provided in the Privacy Act.

To assist in ensuring compliance with the Privacy Act, it is generally recommended that employers implement clear policies governing the collecting, storage, security, use and disclosure of employees' personal information.

4. For how long must an employer retain an employee's personal data? What is best practice?

An employer must not retain personal information for longer than is required for the purposes for which the information may lawfully be used (in accordance with IPP 9).

However, the Employment Relations Act 2000 requires employers to keep detailed records to demonstrate that the employer has complied with minimum entitlement provisions (e.g., holiday pay and sick leave entitlements ("**wage and time records**")). Wage and time records must be held for six years and must include:

- the name of the employee;
- the employee's age;





New Zealand

In Detail

- the employee’s postal address;
- the kind of work on which the employee is usually employed;
- whether the employee is employed under an individual employment agreement or a collective agreement, and the employee’s classification under it;
- the number of hours worked each day in a pay period and the pay for those hours;
- the wages paid to the employee for each pay period and the method of calculation;
- details of any employment relations education leave; and
- such other particulars as may be prescribed.

Employees’ tax records must be held for seven years before they are destroyed. In relation to other personal information, best practice is to obtain an employee’s written consent to retain information for a specified period and then securely destroy personal information as soon as it is no longer required.

5. What are the legal restrictions on transferring employees’ personal data outside your jurisdiction?

An employer is prohibited from using or disclosing employees’ personal information for any other purpose or in any other way than that which was notified to the employee at the time the information was collected.

Strictly speaking, employees’ express consent is required for any use and/or disclosure that were not notified to them at the time their personal information was collected (in accordance with IPP 3).

Section 10 of the Privacy Act deals with the application of information privacy principles to information held overseas:

- Principles relating to storage and security, accuracy, retention, and limits on use and disclosure will apply to information held by an employer outside of New Zealand, where the information has been transferred out of New Zealand by that employer (or any other agency).
- Principles relating to employees’ rights of access to and correction of their personal information apply to all information an employer holds outside of New Zealand.





New Zealand

In Detail

In addition, section 114B of the Privacy Act provides that the Commissioner may prohibit the transfer of personal information from New Zealand to another State, if the Commissioner is satisfied on reasonable grounds that:

- the information has been, or will be, received in New Zealand from another State (defined to include not only countries but also parts of countries, such as states in Australia, provinces in Canada and Hong Kong);
- the information is likely to be transferred from New Zealand to a third State, where it will not be subject to laws providing comparable safeguards to the Privacy Act; and
- the transfer is likely to lead to a contravention of the basic principles of national application set out in Part Two of the OECD Guidelines.

A proposed amendment to the Privacy Act by the Privacy Bill is the strengthening of Cross-Border Data Flow Protections. If enacted in its current form, this would require New Zealand agencies to take reasonable steps to ensure personal information sent/disclosed overseas meets acceptable privacy standards. In general, under the Privacy Bill, personal information would not be able to be disclosed to an overseas person unless:

- the individual concerned consents to the disclosure of his/her information to the overseas person;
- the overseas person is in a country that is prescribed in regulations as having privacy laws comparable to New Zealand; or
- the agency believes that the overseas person is required to protect the information in a way that is comparable to the protections afforded by New Zealand legislation (for example, when there is an agreement where the overseas person will provide such comparable safeguards).

The Bill also makes it clear that a New Zealand organization still needs to comply with New Zealand privacy laws when engaging an overseas service provider.

6. What are the legal restrictions on transferring employees' personal data to a third party?

There is no specific restriction on the transfer of personal information to third parties. Rather, to ensure compliance with IPP 3, an agency must, among other things, ensure that individuals are made aware of all intended recipients of their





New Zealand

In Detail

personal information at the time it is collected. If individuals are not provided with these details at the time that the information is collected (under IPP 3), they will need to specifically consent to the transfer of their personal information (under IPPs 10 and 11).

7. What are the consequences of breaching privacy laws in your jurisdiction?

Privacy Commissioner

An employee who believes there has been an interference with his/her privacy may lodge a complaint with the Privacy Commissioner.

However, if a breach of privacy is found by the Privacy Commissioner, the remedies available are limited to a non-binding recommendation and publicly naming the employer who has breached the Privacy Act. The Privacy Commissioner may also refer the matter to the Director of Human Rights Proceedings, who will determine whether or not to institute proceedings before the Human Rights Review Tribunal.

Administrative Penalties

A person commits an offense and is liable on summary conviction to a fine not exceeding NZD 2,000, who:

- without reasonable excuse, obstructs, hinders or resists the Privacy Commissioner or any other person in the exercise of their powers under the Privacy Act;
- without reasonable excuse, refuses or fails to comply with any lawful requirement of the Privacy Commissioner or any other person under the Privacy Act;
- makes any other statement or gives any information to the Privacy Commissioner or any other person exercising powers under the Privacy Act knowing that the statement or information is false or misleading; or
- represents, directly or indirectly, that he/she holds any authority under the Privacy Act, when he/she does not hold that authority.





New Zealand

In Detail

Human Rights Review Tribunal

An employee may take an action for interference with his/her privacy in the Human Rights Review Tribunal. The remedies that may be sought include:

- a declaration that the action of the defendant is an interference with the privacy of an individual; and
- an order restraining the defendant from continuing or repeating the interference or from engaging in, or causing or permitting others to engage in, conduct of the same kind as that constituting the interference or conduct of any similar kind specified in the order.

The Human Rights Review Tribunal may also award damages for:

- pecuniary loss;
- loss of any benefit (whether or not of a monetary kind);
- humiliation, loss of dignity or injury to feelings of the aggrieved individual (up to a maximum of NZD 350,000);
- an order that the defendant take specified remedial action; or
- such other relief as the Human Rights Review Tribunal thinks fit.

Privacy Bill

The Privacy Bill proposes a number of amendments to the consequences of breaching privacy laws in New Zealand. If enacted, the Privacy Commissioner will have the power to make binding decisions on complaints relating to access to personal information (instead of the current process where the Privacy Commissioner refers such complaints to the Tribunal). In particular, if an employer refuses an individual's request to access his/her personal information, the Privacy Commissioner will be able to direct that employer to make that information available.

New criminal offenses have also been introduced under the Privacy Bill. If enacted, it will be an offense for a person to:

- make or give any false or misleading statements or information to the Privacy Commissioner or other persons exercising powers under the Privacy Act;





New Zealand

In Detail

- falsely represent that he/she has authority under the Privacy Act;
- impersonate or falsely pretend to be an individual for the purposes of obtaining access to that individual's personal information or having that individual's personal information used, altered or destroyed; and
- knowingly destroy documents containing personal information that is the subject of a request.

Any person who commits any of the above offenses will be liable to a fine of up to NZD 10,000.

8. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee's personal data?

The common pitfalls include:

- the failure to properly notify an individual about the collection of personal information (in accordance with IPP 3);
- the use of personal information for a purpose other than that for which it was obtained (prohibited by IPP 10); and
- improper disclosure of personal information (prohibited by IPP 11).

The introduction of the Privacy Bill will be a key area to watch out for in New Zealand. Fundamental aspects of the Privacy Act, such as the IPPs, which regulate the collection, use and disclosure of personal information, are retained, but the Bill introduces new ways to enforce those principles, including more substantive fines and greater powers for the Privacy Commissioner. It is anticipated that, if enacted, changes would take effect in late 2019.

Contributed by: **Carl Blake**, Simpson Grierson



[Link to biography >](#)



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



Pakistan

Contributed by: **Meer & Hasan**



In Brief



In Detail

Contributed by: **Zeeshan Ashraf Meer**, Meer & Hasan



[Link to biography >](#)



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



Pakistan

In Brief

1. Is there a law regulating applicant personal data?

There is no specific law regulating applicant personal data.

2. Is there a law regulating employee personal data?

There is no statutory law, regulation or code that deals with the collection, use and/or handling of an employee's personal data in Pakistan.

3. Do I need to have a privacy statement or agreement?

Although not required, it is recommended that employers have a privacy agreement.

4. How long must I retain employee data? What is best practice?

There is no minimum or maximum legal requirement for how long an employer must hold an employee's personal data. Employers may wish to retain applicant and employee data for at least three years as a precaution in case an action is brought.

5. Can I transfer employee data overseas?

There are no legal restrictions on transferring an employee's personal data outside Pakistan.

6. Can I transfer employee data to a third party?

There is no legal restriction on transferring an employee's personal data to a third party unless there is an agreement to the contrary.

7. What are the consequences of breach?

There are no privacy laws in Pakistan so a breach cannot arise. If, however, privacy agreements are breached, then a civil action for damages may be brought.

8. What are the main pitfalls?

At present, the absence of laws regarding employee's personal data is the main challenge in Pakistan.





Pakistan

In Detail

1. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant’s personal data in your jurisdiction?

There is no specific law regulating applicant personal data.

Please note, however, that the Constitution of Pakistan prohibits discrimination on the basis of union affiliations and political views. Employers should therefore not collect or process such data about applicants. In general, any information collected or processed by employers about applicants must be used strictly for the purposes for which it has been obtained, and adequate measures must be taken to protect the data.

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee’s personal data in your jurisdiction?

At present, there is no statutory law, regulation or code which deals with the collection, use and/or handling of an employee’s personal data in Pakistan.

However, all employers normally require personal data of their employees for security and cross-reference reasons. Moreover, the employee’s name, Computerized National Identification Card and address are also used for filing annual returns. The general principles of the law of tort will apply but they do not require any strict compliance, and lack of malice on the part of the employer in collecting, storing and disclosing the personal data of an employee will be a sufficient defense to any potential action against the employer. Although such an action is a possibility, it is seldom brought.

3. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee’s personal data?

There is no legal requirement to have a document to deal with the employee’s personal data. However, it is recommended that employers implement a privacy policy or agreement.

4. For how long must an employer retain an employee’s personal data? What is best practice?

There is no minimum or maximum legal requirement for how long an employer must hold an employee’s personal data. The employers may wish to retain the employee’s data for at least three years as a precaution in case an action is brought.





Pakistan

In Detail

5. What are the legal restrictions on transferring employees' personal data outside your jurisdiction?

There are no legal restrictions on transferring an employee's personal data outside Pakistan.

6. What are the legal restrictions on transferring employees' personal data to a third party?

At present, there is no statutory law that deals with, controls and regulates the collection and use of handling an employee's personal data in Pakistan; therefore, there is no legal restriction on transferring an employee's personal data to a third party. However, there is one exception and that is if the employee and employer have entered into a confidentiality agreement. Where this is the case, both the parties would be governed by the terms of the confidentiality agreement.

7. What are the consequences of breaching privacy laws in your jurisdiction?

There are no privacy laws in Pakistan so a breach cannot arise. If, however, privacy agreements are breached, then a civil action for damages may be brought.

8. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee's personal data?

At present, the absence of laws regarding an employee's personal data is the main challenge in Pakistan. However, if the personal data disclosed to a third party proves to be incorrect, an action for damages may be brought. This rarely occurs but is still a possibility.

Contributed by: **Zeeshan Ashraf Meer**, Meer & Hasan

 [Link to biography >](#)



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



PRC



Contributed by: **Jingtian & Gongcheng**



In Brief



In Detail

Contributed by: **Deng Youping**, Jingtian & Gongcheng



[Link to biography >](#)



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



PRC

In Brief

1. Is there a law regulating applicant personal data?

There is no specific law regulating applicant personal data. However, there are laws and rules regulating the personal data of general citizens, such as the General Rules of Civil Law, the Criminal Law and the Interpretations on Several Issues concerning the Application of Law in the Handling of Criminal Cases Involving Infringement of Citizens' Personal Information.

2. Is there a law regulating employee personal data?

Yes. The Provisions on Employment Service and Employment Management (revised by the Ministry of Human Resources and Social Security on April 30, 2015).

3. Do I need to have a privacy statement or agreement?

Yes.

4. How long must I retain employee data? What is best practice?

The law is unclear on this subject. We suggest three years as best practice.

5. Can I transfer employee data overseas?

Generally no, unless the employee has provided his/her written consent. If the transfer is to be done via the Internet, a security assessment by the national cyberspace administration authority may be required.

6. Can I transfer employee data to a third party?

Yes, but only with the employee's written consent.

7. What are the consequences of breach?

The most severe consequences are fixed-term imprisonment for not more than three years or criminal detention and/or a fine, if the breach constitutes a crime.

8. What are the main pitfalls?

An employer should keep the personal information of applicants and employees confidential and obtain their written consent or agreement if it will be collecting, transferring or publicizing such personal information.





PRC

In Detail

1. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant’s personal data in your jurisdiction?

There is no specific law regulating applicant personal data. However, there are laws and rules regulating the personal data of general citizens, such as the General Rules of Civil Law (promulgated on March 15, 2017), the Criminal Law (revised in 2017) and the Interpretations on Several Issues concerning the Application of Law in the Handling of Criminal Cases Involving Infringement of Citizens’ Personal Information (jointly promulgated by the Supreme People’s Court and the Supreme People’s Procuratorate on May 8, 2017).

The General Rules provide that “any organization or individual shall legally obtain the personal information of others when necessary and ensure the safety of such personal information, and shall not illegally collect, use, process or transmit the personal information of others, or illegally buy or sell, provide or make public the personal information of others.” The Criminal Law provides that “anyone who sells or illegally provides personal information on citizens to others in violation of the State’s provisions and where the circumstances are serious, shall be sentenced to fixed-term imprisonment for not more than three years or criminal detention, and/or be fined.”

Pursuant to the Interpretation, the term “personal information” mentioned in the Criminal Law refers to “all kinds of information recorded by electronic means or otherwise that can be used independently or together with other information to identify a particular natural person’s identity or reflect particulars on his or her activities, including the natural person’s name, ID number, contact information about his or her e-mail address or phone number, address, account name and password thereof, property conditions, whereabouts and tracks, etc.”

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee’s personal data in your jurisdiction?

Yes. The Provisions on Employment Service and Employment Management (revised by the Ministry of Human Resources and Social Security on April 30, 2015) provide that “employers shall keep confidential the personal data of employees” and that “any publicity of personal data of employees and any use of employees’ techniques and intellectual achievements shall be subject to the written consent of employees.”





PRC

In Detail

3. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee’s personal data?

Pursuant to the Interpretations on Several Issues concerning the Application of Law in the Handling of Criminal Cases Involving Infringement of Citizens’ Personal Information, the act of providing any other individual with any citizen’s personal information legally collected without the consent of the citizen whose personal information is collected shall be deemed as “one providing citizens’ personal information” as mentioned in the Criminal Law (and may therefore be regarded as a crime and subject to penalties). The employer should therefore obtain the employee’s written consent or agreement for its dealing with the employee’s personal data.

4. For how long must an employer retain an employee’s personal data? What is best practice?

There are no clear legal provisions on this subject. However, in our view, it is good practice for an employer to keep its employees’ personal information for three years or more after termination of such employees’ employment.

5. What are the legal restrictions on transferring employees’ personal data outside your jurisdiction?

The transfer of employees’ personal data overseas without their consent may be regarded as “publicizing” and/or “providing any other individual with any citizen’s personal information,” and such act may therefore be deemed in violation of the Provisions on Employment Service and Employment Management and even the Criminal Law where the circumstances are serious. In addition, as provided in the Cyber Security Law (which came into force on June 1, 2017), personal information and important data gathered and produced by key information infrastructure operators during operations shall be stored within the territory of mainland China, and, where it is really necessary to provide such information and data to overseas parties due to business requirements, a security assessment shall be conducted in accordance with the measures formulated by the national cyberspace administration authority.

6. What are the legal restrictions on transferring employees’ personal data to a third party?

Under the Interpretations on Several Issues concerning the Application of Law in the Handling of Criminal Cases Involving Infringement of Citizens’ Personal Information, the act of providing any other individual with any citizen’s personal information legally collected without the consent of the citizen whose personal information is collected may be deemed as “one providing citizens’ personal information” as mentioned in the Criminal Law. So, in the absence of an employee’s written consent, transferring his/her personal information to a third party may be regarded as a crime if the circumstances are serious.





PRC

In Detail

7. What are the consequences of breaching privacy laws in your jurisdiction?

The Provisions on Employment Service and Employment Management do not provide clear consequences of breach in relation to personal information privacy. But, pursuant to the Interpretations on Several Issues concerning the Application of Law in the Handling of Criminal Cases Involving Infringement of Citizens' Personal Information, "any act in violation of the provisions on the protection of citizens' personal information as stipulated in laws, administrative regulations or department rules shall be deemed as "one violating relevant provisions of the State" as mentioned in Article 253A of the Criminal Law," which means the breach may be regarded as a crime where the circumstances are serious, and the consequences thereof may be fixed-term imprisonment for not more than three years or criminal detention and/or a fine.

8. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee's personal data?

An employer should keep the personal information of applicants and employees confidential and obtain their written consent or agreement if it plans to collect, transfer or publicize such personal information.

Contributed by: **Deng Youping**, Jingtian & Gongcheng



[Link to biography >](#)



HOME



COUNTRIES



DIRECTORY

August 2018



Philippines



Contributed by: **Romulo Mabanta Buenaventura Sayoc & de los Angeles**



In Brief



In Detail

Contributed by: **Enriquito J. Mendoza**, Romulo Mabanta Buenaventura Sayoc & de los Angeles



[Link to biography >](#)



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



Philippines

In Brief

1. Is there a law regulating applicant personal data?

Yes, an applicant’s personal data are protected by Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012 (“DPA”).

2. Is there a law regulating employee personal data?

Yes, an employee’s personal data are protected by the DPA.

3. Do I need to have a privacy statement or agreement?

Yes. Employers should have a set of data protection policies that provides for organization, physical and technical security measures and, for such purpose, takes into account the nature, scope, context and purposes of the processing, as well as the risks posed to the rights and freedoms of data subjects.

4. How long must I retain employee data? What is best practice?

Personal data should not be retained for longer than necessary for the:

- (a) fulfillment of the declared, specified and legitimate purpose or when the processing relevant to the purpose has been terminated;
- (b) establishment, exercise or defense of legal claims; or
- (c) legitimate business purposes, which must be consistent with standards followed by the applicable industry or approved by the appropriate government agency.

There is no best practice *per se*. The DPA is relatively new, and practice in this area is still developing. Furthermore, best practice will ultimately be driven by the relevant industry.

5. Can I transfer employee data overseas?

Yes, for the purposes of processing, subject to cross-border arrangements and cooperation and certain conditions.

6. Can I transfer employee data to a third party?

Yes, for the purposes of processing, subject to certain conditions with respect to accountability and provision of consent by the data subject.

7. What are the consequences of breach?

Depending on the nature of the breach, penalties may be in the form of fines of up to PHP 5,000,000, imprisonment of up to six years or both.

8. What are the main pitfalls?

There are none *per se*. As long as the personal data are used for the purpose for which they were obtained, this should be compliant with the law.





Philippines

In Detail

1. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant’s personal data in your jurisdiction?

Yes, an applicant’s personal data are protected by Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012 (“**DPA**”), which was signed into law on August 15, 2012.

The DPA applies to the processing of personal data by any natural or juridical person, whether in the private sector or the government, regardless of whether it is engaged in or outside of the Philippines if:

- (a) The natural or juridical person involved in the processing of personal data is found or established in the Philippines;
- (b) The act, practice or processing relates to personal data about a Philippine citizen or Philippine resident;
- (c) The processing of personal data is being done in the Philippines; or
- (d) The act, practice or processing of personal data is done or engaged in by an entity with links to the Philippines, with due consideration to international law and comity, such as, but not limited to, the following:
 - (i) use of equipment located in the country or maintenance of an office, branch or agency in the Philippines for processing of personal data;
 - (ii) a contract is entered into in the Philippines;
 - (iii) a juridical entity is unincorporated in the Philippines but has central management and control in the country;
 - (iv) an entity that has a branch, agency, office or subsidiary in the Philippines and the parent or affiliate of the Philippine entity has access to personal data;
 - (v) an entity that carries on business in the Philippines; and
 - (vi) an entity that collects or holds personal data in the Philippines.





Philippines

In Detail

Since the passage of the DPA into law, employers have become more conscious about handling the personal information of job applicants and providing consent forms to them in relation to the processing of their personal data.

As a result of this, applications for employment as well as employment contracts now contain explicit provisions that the applicant/employee allows the employer to access, organize, store, consolidate, use, transfer and otherwise process his/her personal information for employment-related purposes, including the evaluation of his/her application for employment. They also contain a statement informing the applicant/employee of his/her rights in relation to the processing of personal data, including the right to information, object, access, rectify, erase or block, damages, data portability, and to file a complaint, as the case may be. Confirmation that the employer will dispose of the applicant's/employee's personal information in a secure manner as soon as the employer determines that it is no longer necessary for the purpose for which it was collected is likewise provided.

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee's personal data in your jurisdiction?

Yes, an employee's personal data are protected by the DPA. Please see response to question 1 for further information.

3. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee's personal data?

Any company involved in the processing of personal data must have a set of data protection policies that provides for organization, physical and technical security measures and, for such purpose, takes into account the nature, scope, context and purposes of the processing, as well as the risks posed to the rights and freedoms of data subjects.

Furthermore, a data subject (e.g., an employee) must be notified and furnished with the information listed below before his/her personal data are entered into the processing system of the personal information collector (e.g., the employer), namely:

- (a) a description of the personal data to be entered into the system;
- (b) the purposes for which the data are being or will be processed, including processing for direct marketing, profiling or historical, statistical or scientific purposes;
- (c) the basis of processing, when processing is not based on the consent of the data subject;





Philippines

In Detail

- (d) the scope and method of the personal data processing;
- (e) the recipients or classes of recipients to whom the personal data are or may be disclosed;
- (f) the methods utilized for automated access, if allowed by the data subject, and the extent to which such access is authorized, including meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
- (g) the identity and contact details of the personal data controller or its representative;
- (h) the period for which the information will be stored; and
- (i) the existence of their rights as data subjects, including the right to access, correction, and object to the processing, as well as the right to lodge a complaint before the Commission.

Finally, a personal information controller/processor employing at least 250 employees must register its data processing system with the National Privacy Commission.

4. For how long must an employer retain an employee’s personal data? What is best practice?

Under the Implementing Rules and Regulations of the DPA (“**IRR-DPA**”), personal data shall not be retained for longer than necessary for the:

- (a) fulfillment of the declared, specified and legitimate purpose, or when the processing relevant to the purpose has been terminated;
- (b) establishment, exercise or defense of legal claims; or
- (c) legitimate business purposes, which must be consistent with standards followed by the applicable industry or approved by the appropriate government agency.

Note that personal data may not be retained in perpetuity in contemplation of a possible future use yet to be determined.





Philippines

In Detail

There is no best practice *per se*. The DPA is relatively new, and practice in this area is still developing. Furthermore, best practice will ultimately be driven by the relevant industry, so that the best practice of an entity that continuously recruits employees (such as business processing outsourcing) may be different from an entity that does not recruit on a continuous basis.

5. What are the legal restrictions on transferring employees' personal data outside your jurisdiction?

Please see response to question 6 below.

6. What are the legal restrictions on transferring employees' personal data to a third party?

The DPA and the IRR-DPA allow the transfer of personal data to third parties for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

In such a case, the personal information controller shall remain accountable for complying with the requirements of the DPA and the IRR-DPA and shall use contractual or other reasonable means to provide a comparable level of protection to the personal data while they are being processed by a personal information processor or third party.

The data subject must give his/her consent to the data sharing before the data are transferred to a third party. The following conditions must also be complied with:

- (a) Consent for data sharing shall be required even when the data are to be shared with an affiliate or parent company or other related companies; and
- (b) Data sharing for commercial purposes, including direct marketing, shall be covered by a data sharing agreement:
 - (i) The data sharing agreement shall establish adequate safeguards for data privacy and security and uphold rights of data subjects;
 - (ii) The data sharing agreement shall be subject to review by the Commission, on its own initiative or upon a complaint from a data subject;





Philippines

In Detail

- (c) The data subject shall be provided with the following information prior to collection or before the data are shared:
- (i) The identity of the personal information controllers or personal information processors that will be given access to the personal data;
 - (ii) The purpose of data sharing;
 - (iii) The categories of personal data concerned;
 - (iv) The intended recipients or categories of recipients of the personal data;
 - (v) The existence of the rights of data subjects, including the right to access and correction, and the right to object; and
 - (vi) Other information that would sufficiently notify the data subject of the nature and extent of data sharing and the manner of processing.
- (d) Further processing of shared data shall adhere to the data privacy principles laid down in the DPA and the IRR-DPA.

7. What are the consequences of breaching privacy laws in your jurisdiction?

There are various penalties arising from a breach of privacy laws.

For example, in relation to the “*unauthorized processing of personal information and sensitive personal information*”:

- A penalty of imprisonment ranging from one year to three years and a fine of not less than PHP 500,000 but not more than PHP 2,000,000 shall be imposed on persons who process personal information without the consent of the data subject or without being authorized under the DPA or any existing law.
- A penalty of imprisonment ranging from three years to six years and a fine of not less than PHP 500,000 but not more than PHP 4,000,000 shall be imposed on persons who process sensitive personal information without the consent of the data subject or without being authorized under the DPA or any existing law.





Philippines

In Detail

Further penalties of imprisonment and fines arise from other breaches, including:

- accessing personal information and restrictive personal information due to negligence;
- improper disposal of personal information and sensitive personal information;
- processing of personal information and sensitive personal information for unauthorized purposes;
- unauthorized access or intentional breaches;
- concealment of security breaches involving sensitive personal information;
- malicious disclosure; and
- unauthorized disclosure.

8. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee's personal data?

There are none *per se*. As long as the personal data are used for the purpose for which they were obtained, this should be compliant with the law.

One gray area in the Philippines is the release of personal data of employees to prospective acquirers of a company for due diligence purposes. Such release of information is not, strictly speaking, for the benefit of the employee. Whether or not this is allowed has still not been fully tackled by the proper authorities.

Contributed by: **Enriquito J. Mendoza**, Romulo Mabanta Buenaventura Sayoc & de los Angeles



[Link to biography >](#)



HOME



COUNTRIES



DIRECTORY

August 2018



Singapore



Contributed by: **Rajah & Tann Singapore LLP**



In Brief



In Detail

Contributed by: **Kala Anandarajah**, Rajah & Tann Singapore LLP



[Link to biography >](#)



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



Singapore

In Brief

1. Is there a law regulating applicant personal data?

Yes. Applicant personal data are regulated by the Personal Data Protection Act 2012 (No. 26 of 2012) (“PDPA”), the overarching data protection legislation in Singapore.

2. Is there a law regulating employee personal data?

Yes. Employee personal data are regulated by the PDPA as well.

3. Do I need to have a privacy statement or agreement?

Yes. Under the PDPA, an organization is required to, among other things, formulate and implement policies and practices that are necessary for it to meet its obligations under the PDPA. Separately, consent is required before an organization may collect, use or disclose personal data about an individual, unless otherwise exempted under the PDPA.

4. How long must I retain employee data? What is best practice?

The period for which employee data must be retained depends on applicable legislation and generally varies between five and seven years.

5. Can I transfer employee data overseas?

Yes, provided that the organization transferring the data complies with the requirements under the PDPA and any personal data transferred is protected to a standard comparable to that under the PDPA.

6. Can I transfer employee data to a third party?

Yes. If employee data are transferred to a third party for the purpose of managing or terminating employment relationships, no consent is required for such transfer, but the employer must notify the employees concerned of the purposes of such transfer. Consent from the employee may be required in other situations unless exempted under the PDPA. Even when employee data are transferred to and processed by a third party, the employer is still subject to the obligations under the PDPA in respect of such data.

7. What are the consequences of breach?

If an organization is found to be in violation of any provision of the PDPA, the organization may be directed to take any remedial measures to ensure compliance with the PDPA, including paying a financial penalty of up to SGD 1 million.

8. What are the main pitfalls?

Many organizations fail to take steps to ensure that a data intermediary (third party) that processes personal data on their behalf adopts appropriate security measures to protect such personal data. It is important to keep in mind that the organization remains responsible and must continue to comply with its obligations under the PDPA in respect of personal data belonging to the organization that is transferred to and processed by a third party.

Employers can potentially be held vicariously liable for any breach of the PDPA provisions by employees who are acting in the course of their employment, whether or not such act was done with the employer’s knowledge or approval. Hence, employers should provide training in relation to compliance with the PDPA to their employees.



Singapore

In Detail

1. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant’s personal data in your jurisdiction?

The Personal Data Protection Act (“**PDPA**”), along with its subsidiary legislation, regulates the collection, use and/or disclosure of personal data in Singapore, including applicants’ personal data. The PDPA is administered and enforced by the Personal Data Protection Commission (“**PDPC**”).

Personal data are defined under the PDPA as data, whether true or not, about an individual who can be identified from that data or from that data and other information to which the organization has or is likely to have access.

The term “organization” includes any individual, company, association or body of persons, corporate or unincorporated, whether or not:

- (a) formed or recognized under the law of Singapore; or
- (b) resident, or having an office or a place of business, in Singapore.

Under the PDPA, there are nine key obligations relating to the collection, use and disclosure of personal data, as set out by the PDPC in its guidelines:

- (a) the Consent Obligation – to obtain the consent of the individual before collecting, using or disclosing his/her personal data for a particular purpose;
- (b) the Purpose Limitation Obligation – to collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances and, if applicable, have been notified to the individual concerned;
- (c) the Notification Obligation – to notify an individual of the purpose(s) for which it intends to collect, use or disclose the individual’s personal data on or before such collection, use or disclosure;
- (d) the Access and Correction Obligations – upon request, to:





Singapore

In Detail

- (i) provide an individual with his/her personal data in the possession or under the control of the organization and information about the ways in which the personal data may have been used or disclosed during the past year; and
 - (ii) correct an error or omission in such personal data;
- (e) the Accuracy Obligation – to use reasonable efforts to ensure that personal data collected by or on behalf of an organization are accurate and complete if the personal data are likely to be used by the organization to make a decision that affects the individual concerned or be disclosed by the organization to another organization;
- (f) the Protection Obligation – to protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks;
- (g) the Retention Limitation Obligation – to cease to retain documents containing personal data or to anonymize such personal data as soon as it is reasonable to assume that:
 - (i) the purpose for which the personal data were collected is no longer being served by retention of the personal data; and
 - (ii) retention is no longer necessary for legal or business purposes;
- (h) the Transfer Limitation Obligation – not to transfer personal data to a country or territory outside Singapore except in accordance with the requirements prescribed under the PDPA; and
- (i) the Openness Obligation – to implement the necessary policies and procedures to meet its obligations under the PDPA and to make information about its policies and procedures publicly available.

Specifically, in relation to job applicants, where an individual voluntarily provides his/her personal data to an organization through a job application, he/she may be deemed to have consented to the collection, use and disclosure of his/her personal data by the organization for the purpose of assessing the job application. Separately, an organization may collect, use or disclose personal data without consent where this is necessary for evaluative purposes, which is defined under the PDPA to include, among other things, the purpose of determining the suitability, eligibility or qualifications of an individual for employment. This exception would apply in the context of job applications.





Singapore

In Detail

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee's personal data in your jurisdiction?

The PDPA regulates the collection, use and/or handling of all personal data, including employees' personal data.

Under the PDPA, the collection, use and disclosure of employees' personal data for the purpose of managing or terminating their employment relationships do not require the consent of the employees concerned.

Nevertheless, section 20(4) of the PDPA requires an employer, on or before collecting, using or disclosing personal data of an employee for the purpose of managing or terminating the employment relationship, to inform the employee of:

- (a) that purpose; and
- (b) on request by the employee, the business contact information of a person who is able to answer the employee's questions about that collection, use or disclosure on behalf of the employer.

The purposes for the collection, use and disclosure of employees' personal data can be notified to the employees through employment contracts, employee handbooks or notices in the company intranet, whichever is more appropriate in the circumstances.

Employers are still required to seek consent from, and to notify, employees when using their personal data for purposes that are not related to the management or termination of the employment relationship (unless any other exception under the PDPA applies). In any event, an employer will be subject to the other obligations under the PDPA when collecting, using and disclosing its employees' personal data, as set out in the response to question 1 above.

3. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee's personal data?

Yes. Pursuant to Section 12 of the PDPA, an organization is required to:

- (a) develop and implement policies and practices that are necessary for it to meet its obligations under the PDPA;
- (b) develop a process to receive and respond to complaints that may arise with respect to the application of the PDPA;
- (c) communicate to its staff information about its policies and practices referred to in (a) above; and





Singapore

In Detail

(d) make information available on request about the policies and practices referred to in (a) above and the complaint process referred to in (b) above.

Hence, an organization should have a publicly available privacy policy that sets out how it handles personal data.

Separately, under section 13 of the PDPA, an organization may not collect, use or disclose personal data about an individual unless:

- (a) the individual gives, or is deemed to have given, his/her consent under the PDPA to the collection, use or disclosure; or
- (b) the collection, use or disclosure of the personal data without the consent of the individual is required or authorized under the PDPA or any other written law.

While there is no requirement for consent to be given in the form of a written agreement, it is advisable for an organization to keep records of the consents obtained in case there are any disputes in future.

4. For how long must an employer retain an employee's personal data? What is best practice?

The PDPA does not prescribe minimum periods for data retention. In this regard, the organization is advised to retain data for such period that is necessary for it to comply with other applicable legislation in Singapore, which may vary between five to seven years. For example, under the Income Tax Act and the Goods and Services Tax Act, businesses are required to keep their records for at least five years. Hence, as a matter of best practice, and where necessary, an employee's personal data may be retained for up to seven years.

However, section 25 of the PDPA imposes an obligation on organizations to stop retaining personal data or to anonymize such personal data as soon as it is reasonable to assume that:

- (a) the purpose for which that personal data was collected is no longer being served by retention of the personal data; and
- (b) retention is no longer necessary for legal or business purposes.

Therefore, employee personal data cannot be retained for an excessive period of time.





Singapore

In Detail

5. What are the legal restrictions on transferring employees' personal data outside your jurisdiction?

Section 26(1) of the PDPA prohibits the transfer of personal data to a country or territory outside Singapore by an organization, except in accordance with the requirements prescribed under the PDPA, to ensure that such personal data are protected to a standard that is comparable to that under the PDPA.

Based on guidance provided by the PDPC, an organization can transfer personal data overseas if it has taken appropriate steps to ensure that:

- (a) it will comply with its obligations under the PDPA in respect of such personal data while it remains in the possession or under the control of the organization; and
- (b) if the personal data are transferred to a recipient located outside Singapore, such recipient is bound by legally enforceable obligations to protect such personal data to a standard that is comparable to that under the PDPA. In this regard, legally enforceable obligations include obligations imposed on the recipient under:
 - (i) any law;
 - (ii) any contract that requires the recipient to protect such personal data to a standard that is at least comparable to that under the PDPA and specifies the countries and territories to which such personal data may be transferred under the contract; and
 - (iii) any binding corporate rules that:
 - (A) require every recipient of the transferred personal data to protect it to a standard that is at least comparable to that under the PDPA; and
 - (B) specify the recipients of the transferred personal data to which the binding corporate rules apply, the countries and territories to which the personal data may be transferred under the binding corporate rules, and the rights and obligations provided by the binding corporate rules; or
 - (iv) any other legally binding instrument.





Singapore

In Detail

An organization is taken to have satisfied its obligations in relation to the transfer of personal data to a recipient located outside Singapore if:

- (a) the individual consents to such transfer;
- (b) such transfer is necessary for the performance of a contract between the individual and the transferring organization or to do anything at the individual's request with a view to the individual entering into a contract with the transferring organization;
- (c) such transfer is necessary for the conclusion or performance of a contract between the transferring organization and a third party that is entered into at the individual's request;
- (d) such transfer is necessary for the conclusion or performance of a contract between the transferring organization and a third party if a reasonable person would consider the contract to be in the individual's interest;
- (e) such transfer is necessary for the personal data to be used or disclosed in situations where consent of the individual concerned is not required under the PDPA and the transferring organization has taken reasonable steps to ensure that the personal data transferred will not be used or disclosed by the recipient for any other purpose;
- (f) the personal data are data in transit; or
- (g) the personal data are publicly available in Singapore.

Separately, an organization may apply for an exemption from the requirements under section 26(1) of the PDPA from the PDPC in respect of any transfer of personal data by that organization. The PDPC may impose certain conditions on the organization when granting the exemption, which can be revoked at any time by the PDPC.

6. What are the legal restrictions on transferring employees' personal data to a third party?

As stated in our response to question 2, if the transfer or disclosure of the employees' personal data to a third party is for the purpose of managing or terminating their employment relationships, the employer would not be required to obtain their consent for such disclosure. However, the employer must notify the employees of the purpose of such disclosure.





Singapore

In Detail

If the transfer of employees' personal data is for purposes other than managing or terminating their employment relationships, then, subject to certain exceptions under the PDPA, the employer would have to obtain their consent and notify them of such purposes before transferring their personal data to the third party.

In addition, the employer should make reasonable security arrangements to protect the employees' personal data from unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks, as required under section 24 of the PDPA. The measures taken to protect employees' personal data should be reasonable and appropriate in the circumstances (for example, taking into account the nature of the personal data, the form in which it has been collected and the potential impact on the individuals concerned in the event of a data breach).

Before transferring employees' personal data to a third party, the employer should also enter into a written contract with the third party to clearly set out the responsibilities and obligations of the third party with respect to the employee data, including requiring the third party to take appropriate security measures to protect such data as required under the PDPA.

7. What are the consequences of breaching privacy laws in your jurisdiction?

Pursuant to Section 29 of the PDPA, where an organization is in violation of any of its obligations under the PDPA, the PDPC may issue such directions as it thinks fit in the circumstances to ensure compliance with such obligation(s). These directions include requiring organizations to:

- (a) stop collecting, using or disclosing personal data in contravention of the PDPA;
- (b) destroy personal data collected in contravention of the PDPA;
- (c) comply with any direction of the Commission under section 28(2) of the PDPA (relating to access to and correction of personal data); and/or
- (d) pay a financial penalty of up to SGD 1 million.





Singapore

In Detail

8. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee’s personal data?

Many organizations fail to take steps to ensure that a data intermediary (third party) that processes their employees’ personal data on their behalf adopts appropriate security measures to protect such personal data (for example, when outsourcing business functions, such as payroll and employee benefits). It is important to keep in mind that the organization remains responsible for and must continue to comply with its obligations under the PDPA in respect of such personal data, even when it is transferred to and processed by a third party. Hence, organizations should enter into written agreements with third parties to ensure that employees’ personal data are adequately protected and used only for purposes that are stipulated by the organization to ensure compliance with the PDPA.

Separately, pursuant to section 53(1) of the PDPA, employers will be held vicariously liable for any breach of the PDPA provisions by its employees who are acting in the course of their employment, whether or not such act was done with the employer’s knowledge or approval. However, it would be a defense for the employer to prove that it took practical steps to prevent the employees from engaging in any act or conduct that resulted in the breach. It is therefore crucial for employers to train their employees, especially those handling personal data, to ensure that they are aware of and comply with their obligations under the PDPA when collecting, using or disclosing any personal data in the course of their employment.

Contributed by: **Kala Anandarajah**, Rajah & Tann Singapore LLP



[Link to biography >](#)



HOME



COUNTRIES



DIRECTORY

August 2018



South Korea



Contributed by: **Kim & Chang**



In Brief



In Detail

Contributed by: **Michael Kim, Joo Hee Kim & Ari Yoon, Kim & Chang**



[Link to biography >](#)



[Link to biography >](#)



[Link to biography >](#)



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



South Korea

In Brief

1. Is there a law regulating applicant personal data?

The Personal Information Protection Act (“**PIPA**”) is the primary general law that regulates the processing of personal data of any living person, including applicants. The Fair Hiring Procedure Act also applies when retaining applicants’ records or returning them to the applicants.

2. Is there a law regulating employee personal data?

As stated above, the PIPA is the primary general law regulating the processing of personal data of any living person, including employees. Further, labor laws, including the Labor Standards Act (“**LSA**”), provide the rules and regulations applicable to employers and employees.

3. Do I need to have a privacy statement or agreement?

The PIPA requires that a privacy policy be publicly disclosed. Further, employers will need the prior explicit consent of officers and employees before they can process their personal data (which is quite broadly defined).

4. How long must I retain employee data? What is best practice?

The LSA requires that an employer retain certain enumerated documents related to the employment relationship for three years. If the employer wishes to retain such records beyond this period, the employer must obtain explicit consent from the relevant employee with certain disclosures made (e.g., the period of time that the employer wishes to retain the employee data).

5. Can I transfer employee data overseas?

Yes. Depending on whether the overseas transfer is a delegation of personal data processing or a third-party provision, either prior consent from an employee (in the case of a third-party provision) or a delegation agreement (among other things) is required (in the case of a delegation of personal data processing).

While the PIPA does not require separate consent for an overseas transfer, in the case of overseas third-party provision, the employer must notify the employee of the country in which the recipient is located (in addition to other mandatory disclosure items for the consent for third-party provision) when obtaining consent for the third-party provision.

6. Can I transfer employee data to a third party?

Please refer to the response to question 5.

7. What are the consequences of breach?

Breaching the PIPA may result in administrative and/or criminal penalties. Further, the employer or company may be subject to a civil action for damages initiated by data subjects (i.e., employees).

8. What are the main pitfalls?

A common pitfall occurs when an employer fails to obtain express or explicit consent from an employee. Implicit consent is not recognized under Korean law, and therefore the employee must clearly give his/her consent. Further, detailed, and potentially onerous, security measures are mandatory under Korean privacy laws to safeguard personal data.



South Korea

In Detail

1. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant’s personal data in your jurisdiction?

The Personal Information Protection Act (“**PIPA**”) is the primary general law that regulates the processing of personal data of any living person, including applicants. The PIPA requires that prior consent be obtained for the collection, use and third-party provision of the applicant’s/employee’s personal data, unless a statutory exception applies. The Fair Hiring Procedure Act would also apply when retaining applicants’ records or returning them to the applicants. Under this law, an unsuccessful applicant may request that his/her application (with his/her personal data) be returned to the applicant within 14 days from the date of request. To handle such requests from unsuccessful applicants, companies are required to set a time period (between 14 and 180 days from the date the decision on the applicant is made) during which unsuccessful applicants may exercise such right.

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee’s personal data in your jurisdiction?

The PIPA is the primary general law regulating the processing of personal data of all living persons, including employees. Further, labor laws, including the LSA, provide rules and regulations applicable to employers and employees.

3. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee’s personal data?

Under the PIPA, an employer handling employee personal data must publicly disclose a privacy policy. Data processors usually abide by this requirement by posting the privacy policy on the home page of the company’s website. The privacy policy must include information on the purpose(s) of processing the personal data, retention period, third-party transfers and delegation.

Further, prior to any collection and use of personal data, the data controller (i.e., the employer) must obtain prior express consent from the employee unless a statutory exemption applies. To enable the employee to give the employer informed consent, the employer must provide the employee with details relating to:

- (1) the personal data being collected;
- (2) the purpose of collection and use;





South Korea

In Detail

- (3) the time period for possession and use of the personal data;
- (4) the employee’s right to refuse to consent; and
- (5) the consequences and/or disadvantages of refusing consent.

More often than not, employers use written consent forms to obtain consent from employees, and the above items are included in such written consent forms.

4. For how long must an employer retain an employee’s personal data? What is best practice?

The PIPA does not specify a detailed retention period, but it requires employers to immediately destroy employee personal data when it becomes unnecessary (e.g., if the purposes for which the personal data were collected have been satisfied) unless the retention of personal data is mandated by other statutes. For instance, the LSA requires employers to retain certain enumerated documents related to the employment relationship for three years after termination of employment. The Ministry of the Interior and Safety (“MOIS”), the primary regulator enforcing the PIPA, recommends that the employer permanently delete employee personal data within five days of the end of the three-year retention period. If the employer needs to retain employee data for the purpose of issuing a work history certificate beyond the three-year period, it must obtain prior consent from the employee.

5. What are the legal restrictions on transferring employees’ personal data outside your jurisdiction?

The PIPA does not require a separate consent to transfer employee personal data overseas. Depending on whether the overseas transfer is (i) a delegation of personal data processing or (ii) a third-party provision, either prior consent from the employee (in the case of a third-party provision) or a delegation agreement (among other things) is required (in the case of a delegation of personal data processing). In the case of an overseas third-party provision, the employer or the company must notify the employee of the country in which the recipient is located (in addition to other mandatory disclosure items for the consent for third-party provision) when obtaining consent for the third-party provision. Please see question 6 for a detailed explanation of “delegation” and “third-party provision” of personal information.

6. What are the legal restrictions on transferring employees’ personal data to a third party?

As noted in question 5, the PIPA distinguishes between the “provision of personal information to third parties” (i.e., third-party provision) and the “delegation of personal information processing.” Although both involve providing personal





South Korea

In Detail

information to another entity, a third-party provision refers to the case in which the company sends personal data to a third party, which then uses the personal data for its own purposes or benefit (for example, Company A provides its employees' personal information to its headquarters for HR management purposes and the headquarters use the personal information not just for HR management purposes but for other purposes as well). Delegation, on the other hand, refers to the case in which the company delegates a specific task to a third-party service provider to perform on its behalf (e.g., payroll services or data processing).

Provision of personal information to third parties

For the provision of personal information to a third party, a company must obtain consent (with a few exceptions) after it notifies an employee of:

- the person/entity to whom the personal data are provided;
- the purpose of use of the personal data by the person/entity;
- the types of personal data provided;
- the period of time during which the person/entity will retain and use the personal data;
- the employee's right to refuse to consent; and
- the consequences or disadvantages of refusing consent.

Under the PIPA, separate consent is not required purely because the data are being transferred overseas. The data transferor can simply state that the data are being provided to an overseas third party and provide the name of the country where the overseas third party resides when it obtains consent for the provision of personal data to a third party.

Delegation of personal information processing

In a delegation context, the PIPA requires a written delegation agreement to be in place between a delegator company (i.e., the employer) and a delegatee company that includes clauses addressing:

- the purpose and scope of the delegation;





South Korea

In Detail

- the limitations on the scope of such delegation (e.g., the prohibition of processing personal data for any other purpose other than the delegated purpose or any limitation on sub-delegations);
- the technical and managerial protective measures;
- the supervision of the delegatee, such as check-ups on the current status of management of personal data possessed in relation to the delegation; and
- the compensation for damages in case of the delegatee company's breach of duties.

In addition, the employer has the duty to disclose to the employee the name of the delegatee company and the delegated task(s). Further, if the employer delegates a service involving the advertisement or sale of goods and services, the name of the delegatee company and the specific delegated task(s) must be notified to the employee through a document, mail, email, facsimile, telephone or text message, or other similar methods. Further, the employer is obliged to train and monitor the delegatee on the safeguarding of the delegated employee personal data. Notwithstanding the above, the PIPA does not require specific consent from the employee for such delegation to take place.

7. What are the consequences of breaching privacy laws in your jurisdiction?

If an individual employee violates the PIPA, he/she may be subject to criminal penalties (imprisonment of up to 10 years or a criminal fine of up to KRW 100 million) and potential civil damages. Similarly, an employer may also be subject to administrative penalties (corrective order, administrative fine of up to KRW 50 million, administrative surcharge of up to KRW 500 million).

8. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee's personal data?

Korea is an opt-in regime where the employees must provide express consent to the processing of their personal data. Implicit consent will not be recognized. As outlined above, detailed disclosures need to be made to employees to enable them to provide informed consent. If any of the disclosure details change, fresh consent will be required.

An employer should also be mindful that consent must be separately and respectively obtained for: (i) the collection and use, (ii) third-party provision (if any), (iii) sensitive personal data, and (iv) unique identification data (please note resident registration numbers are prohibited from being collected unless an exception applies). It is not permissible to have one





South Korea

In Detail

comprehensive consent that covers all of the above items. Further, the personal data must be categorized into either mandatory personal data or optional personal data, each requiring separate consents. Mandatory personal data refer to data that are absolutely necessary to provide the services intended, and optional personal data refer to data that are not, such as data used for marketing purposes. Also, the various purposes for which the personal data are processed must be divided into either mandatory purposes or optional purposes, for which consent must be separately obtained.

Lastly, the PIPA also imposes detailed security measures in order to safeguard personal data. Employers may find these measures onerous. Examples of such security measures are (i) the installation and operation of access restriction systems (such as intrusion prevention systems and intrusion detection systems) for preventing illegal access to and leakage of personal information and (ii) the application of encryption technology to enable the secure storage and transfer of personal information.

Contributed by: **Michael Kim, Joo Hee Kim & Ari Yoon, Kim & Chang**



[Link to biography >](#)



[Link to biography >](#)



[Link to biography >](#)



HOME



COUNTRIES



DIRECTORY

August 2018



Sri Lanka



Contributed by: John Wilson Partners

 In Brief

 In Detail

Contributed by: John Wilson, John Wilson Partners

 [Link to biography >](#)



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Sri Lanka

In Brief

1. Is there a law regulating applicant personal data?

There is no specific overarching general law regulating applicant personal data. However, a remedy for violation of privacy does exist in the common law of Sri Lanka and may be used in appropriate instances. There are certain industry-specific rules, laws and other directives in force that may also be relevant. Data protection legislation/self-regulatory codes are under consideration that may also impact employee personal data.

2. Is there a law regulating employee personal data?

There is no specific overarching general law regulating employee personal data.

3. Do I need to have a privacy statement or agreement?

Generally, no.

4. How long must I retain employee data? What is best practice?

The retention period for employee data will depend on the category of employee.

5. Can I transfer employee data overseas?

Generally, an employer may transfer employee data overseas unless a specific regulatory requirement applies.

6. Can I transfer employee data to a third party?

Generally, an employer can transfer employee data to a third party.

7. What are the consequences of breach?

The consequences of a breach will vary according to the circumstances. Generally, an aggrieved party can bring an action for injury under the *actio iniuriarum* of the Roman-Dutch law principles relating to privacy.

8. What are the main pitfalls?

There is no specific overarching general legal framework regulating applicant or employee personal data in Sri Lanka.





Sri Lanka

In Detail

1. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant's personal data in your jurisdiction?

Currently there is no legislation regulating the collection, use and/or handling of an applicant's personal data in Sri Lanka. Data protection legislation/self-regulatory codes are under consideration that may also impact applicant/employee personal data. However, no Bill has been presented to Parliament yet.

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee's personal data in your jurisdiction?

Currently, there is no legislation regulating the collection, use and/or handling of an employee's personal data in Sri Lanka. Please see response to question 1.

3. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee's personal data?

Generally, there is no obligation on employers to have a document dealing with the personal data of employees.

4. For how long must an employer retain an employee's personal data? What is best practice?

Retention periods depend on the applicable legislation governing the particular category of employee. For example, there are differing retention periods for employment records and service records after termination under the Shop and Office Employees Act. A retention period of four years also applies under the Wages Boards Ordinance.

5. What are the legal restrictions on transferring employees' personal data outside your jurisdiction?

There are no legal restrictions or statutory provisions governing the transfer of employees' personal data outside of Sri Lanka. Specific regulatory requirements may apply (e.g., in connection with a European employer covered by the GDPR that has a subsidiary in Sri Lanka).





Sri Lanka

In Detail

6. What are the legal restrictions on transferring employees' personal data to a third party?

There are no legal restrictions or statutory provisions governing the transfer of employees' personal data to a third party. However, employers should take care to refrain from communicating data which might be defamatory (e.g., information that the employee has been convicted of a criminal offense).

7. What are the consequences of breaching privacy laws in your jurisdiction?

The remedy against a breach of an individual's privacy is found in the Roman-Dutch law (which is the common or residuary law of Sri Lanka) in the form of an action for injury under the *actio iniuriarum*. Damages might lie in the event of success in any action for breach of privacy based on the *actio iniuriarum*. The concept of *actio iniuriarum* is quite restrictive, as many requirements have to be satisfied to succeed in a claim.

In Sri Lanka, there was a recent case related to privacy and freedom of the press (*Sinha Ratnatunge v The State*). In this case, the Supreme Court of Sri Lanka highlighted the importance of an individual's right to privacy.

8. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee's personal data?

The biggest pitfall is that there is currently no general overarching statutory framework regulating applicant or employee personal data in Sri Lanka.

Contributed by: **John Wilson**, John Wilson Partners



[Link to biography >](#)



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



Taiwan

Contributed by: **Lee, Tsai & Partners, Attorneys-at-Law**



In Brief



In Detail

Contributed by: **Chung-Teh Lee & Elizabeth Pai, Lee, Tsai & Partners, Attorneys-at-Law**



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



Taiwan

In Brief

1. Is there a law regulating applicant personal data?

Yes, the Personal Information Protection Act (“PIPA”) regulates the collection, processing and usage of personal information, including that of job applicants. In addition, the Employment Service Act prohibits the collection of private information from a job applicant that is not required for employment against his/her will.

2. Is there a law regulating employee personal data?

Yes, the PIPA regulates employee personal data.

3. Do I need to have a privacy statement or agreement?

No, but the PIPA requires that (1) a private sector employer makes the collected personal data of an employee available to such employee for inspection and review, or provides a duplicate of such personal data upon such employee’s request (subject to certain exceptions, such as national security concerns, etc.) and (2) a notification with certain information should be presented to an employee when the employee’s personal data are collected, used or handled.

4. How long must I retain employee data? What is best practice?

Under the PIPA, in general, an employer may retain an employee’s personal data for as long as the specific purpose for retaining the information exists or the retention period has not expired.

5. Can I transfer employee data overseas?

Yes, subject to the requirements under the PIPA.

6. Can I transfer employee data to a third party?

Yes, subject to the requirements under the PIPA.

7. What are the consequences of breach?

Under the PIPA, employers may be subject to a range of civil, criminal and administrative liabilities if they fail to provide adequate protection for an individual’s right of privacy.

8. What are the main pitfalls?

Employers should take note of any amendments to the law in Taiwan following the EU’s implementation of the General Data Protection Regulation (“GDPR”) on May 25, 2018.





Taiwan

In Detail

1. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant's personal data in your jurisdiction?

Yes, the Personal Information Protection Act (“**PIPA**”) regulates the collection, processing and usage of personal information, including that of job applicants. In addition, the Employment Service Act (“**ESA**”) prohibits the collection of private information from a job applicant that is not required for employment against his/her will.

The PIPA

- A. For the collection and processing of personal information by a private sector employer, except for the information stated in Article 6 of the PIPA (as detailed below), there must be a specific purpose and it should comply with one of the following conditions (Article 19 of the PIPA):
- (1) it is in accordance with law;
 - (2) there is a contractual or quasi-contractual relationship with the individual whose personal information is to be or has been collected, processed or used (“the Party”), and proper security measures have been adopted;
 - (3) the Party has made public such information himself/herself or the information has been publicized legally;
 - (4) it is necessary for public interests on statistics or for the purpose of academic research conducted by a research institution. The information may not lead to the identification of a specific person after being processed by the provider, or from the disclosure by the collector;
 - (5) consent has been given by the Party;
 - (6) it is necessary to promote public interests;
 - (7) the personal information is obtained from publicly available resources. However, this condition does not apply if the information is limited by the Party in relation to the processing or use and the interests of the Party should be protected; and
 - (8) the rights and interests of the Party are not harmed.





Taiwan

In Detail

- B. Except for the information stated in Paragraph 1 of Article 6 of the PIPA (as detailed below), the private sector employer should limit the use of the personal information to the scope of the specific purpose. However, the information may be used outside the scope upon the occurrence of one of the following conditions (Article 20 of the PIPA):
- (1) it is in accordance with law;
 - (2) it is necessary to promote public interests;
 - (3) it is to prevent harm to the life, body, freedom or property of the Party;
 - (4) it is to prevent harm to the rights and interests of other people;
 - (5) it is necessary for public interests on statistics or the purpose of academic research conducted by a government agency or an academic research institution, respectively. The information may not lead to the identification of a specific person after its processing by the provider, or from the disclosure by the collector;
 - (6) consent has been given by the Party; and
 - (7) such use benefits the Party.
- C. In principle, the sensitive personal information specified under Article 6, Paragraph 1 of the PIPA (e.g., medical records, treatment records, genetics information, sexual activity, physical examination results and criminal records) may not be collected, processed or used unless any of the following circumstances applies (Article 6 of the PIPA):
- (1) when it is in accordance with law;
 - (2) when it is necessary for a government agency to perform its legal duties or for a private sector employer to fulfill its legal obligation, and proper security measures are adopted prior or subsequent to such collection, processing or use;
 - (3) when the Party has made public such information himself/herself or the information concerned has been publicized legally;





Taiwan

In Detail

- (4) where it is necessary to perform statistical or other academic research, a government agency or an academic research institution collects, processes or uses personal information for the purpose of medical treatment, public health or crime prevention. The information may not lead to the identification of a specific person after its processing by the provider or from the disclosure by the collector;
- (5) where it is necessary to assist a government agency in performing its legal duties or a private sector employer in fulfilling its legal obligations, and proper security measures are adopted prior or subsequent to such collection, processing or use; and
- (6) where the Party has consented in writing unless:
 - (i) such consent exceeds the necessary scope of the specific purpose;
 - (ii) the collection, processing or use with the consent of the Party is prohibited by other statutes; or
 - (iii) such consent is against the Party's will.

Employment Service Act

Article 5, Paragraph 2 of the ESA states that, with respect to an employer's collection of an applicant's or employee's personal information, the employer may not withhold the National ID card, work identification or other identification documents of any job applicant or employee or otherwise request applicants or employees to provide private information that is not needed for employment against their will.

According to Article 5, Paragraph 2 of the ESA and Article 1-1, Paragraph 2 of the Enforcement Rules thereof, when the employers collect personal information from job applicants, the rights and interests of the job applicants concerned shall be respected. The collection shall not exceed the specific purpose of economic necessity and public interest maintenance and shall have a legitimate and reasonable connection with the purpose.

The information stipulated in Article 8 of the PIPA (see below) should be provided before collection but it is not necessary to obtain consent from the job applicant for the collection of non-sensitive personal information due to the quasi-contractual relationship of applicant/employer.





Taiwan

In Detail

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee’s personal data in your jurisdiction?

The law relating to the collection, use and/or handling of an applicant’s personal data is applicable to the collection, use and/or handling of an employee’s personal data. Please refer to question 1 above.

3. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee’s personal data?

There is no legal requirement to have a document, such as a privacy policy, to deal with the use of an employee’s personal data. However, the PIPA requires a private sector employer to make the collected personal data of an employee available to such employee for inspection and review or to provide a duplicate of such personal data upon such employee’s request (subject to certain exceptions, such as national security concerns, etc.). In addition, the PIPA imposes an obligation on a private sector employer to specifically notify an employee of certain information, as stated in Article 8 below, when the employer collects such employee’s non-sensitive personal data from him/her either directly or indirectly.

A. Notice to employees when collecting non-sensitive personal data

(A) According to Article 8 of the PIPA, when a private sector employer collects an employee’s non-sensitive personal data for a specific purpose directly from the employee due to one of the circumstances prescribed in Article 19 of the PIPA (i.e., circumstances listed under question 1 above), the employee shall be explicitly notified of the following information:

- (1) the name of the private sector employer;
- (2) the purpose of collection;
- (3) the types of personal data;
- (4) the time period (retention period), the area and manner of the personal data to be used, and the entity(ies) that will use the personal data;





Taiwan

In Detail

(5) the employee's rights to and manners to exercise his/her personal data under Article 3 of the PIPA. Those rights (i.e., rights to inspect, inquire or view, to request a duplicate, to request the supplementation or correction of the information, to request for discontinuance of collection, handling or use, and to request deletion) may not be waived or otherwise restricted in advance; and

(6) the employee's right not to provide his/her personal data and the impact of exercising this right.

(B) However, if any of the following circumstances applies, the requirement for an employer to notify its employee of the information above may be exempted:

- (1) such notification is not required by law;
 - (2) it is necessary for the employer to perform its statutory obligations;
 - (3) the notification will undermine a public sector body's performance of its statutory duty;
 - (4) the notification will impair public interests;
 - (5) the employee should have known the content of the notification; or
 - (6) when the collection of personal information is for nonprofit purposes and clearly does not cause any detriment to the Party.
- (C) On the other hand, according to Article 9 of the PIPA, when a private sector employer has an employee's non-sensitive personal data for a specific purpose from a third party due to the enumerated circumstances prescribed in Article 19, prior to the handling or use of such personal data, in addition to items (1) to (5) out of the six types of information that shall be explicitly notified to the employee as described in paragraph A(A) above, the source of obtaining such personal data shall also be stated in the notification, subject to certain exceptions (e.g., where one of the above exemptions applies).

B. Collecting, handling and using employees' sensitive personal data

As stated in our response to question 1, it is in principle prohibited to collect, process or use the sensitive personal information listed under Article 6 of the PIPA; if the exceptional circumstances listed under Article 6 of the PIPA apply





Taiwan

In Detail

and the employer is allowed to collect, process or use such information, the employer must still follow the relevant restrictions set under Article 6, Paragraph 1 of the PIPA as well as comply with (A), (B) and (C) above under question 3A.

4. For how long must an employer retain an employee's personal data? What is best practice?

Under the PIPA, an employer, in general, may retain an employee's personal data for as long as any of the specific purposes exists or the period of retention has not expired. According to Article 11, Paragraph 3 of the PIPA, once the employer no longer needs to collect the personal data under the specific purpose or the retention period for the relevant personal data (as notified to the employee when collecting the employee's personal data) has expired, the employer shall actively, or upon the employee's request, delete or discontinue handling or using such employee's personal data. However, where it is necessary for the performance of business or the employee has consented in writing, the employer may still retain, handle or use the employee's personal data.

As such, under the PIPA, the best practice for retaining, handling and using an employee's personal data after the purpose for collecting such information ceases to exist or the informed retention period has expired will be to ask the employee expressly to consent to such retention in a written agreement.

5. What are the legal restrictions on transferring employees' personal data outside your jurisdiction?

Should the employer intend to transfer non-sensitive personal information outside the country for processing and use, unless the circumstances listed in our response to question 3A(B) are met, the employees shall be notified, pursuant to Article 8 of the PIPA, of the intended transfer at the time of the collection of the information. In addition, the act of processing or using personal information outside the country must still be within the scope of necessity for the specific purpose that the employer is collecting such information.

As for sensitive personal information, following the response to question 3, such information may only be collected, processed or used if the circumstances under Article 6, Paragraph 1 of the PIPA are met. If an employer meets such requirements and intends to transfer such information outside of the country for processing or use, in addition to the requirements under Article 6, Paragraph 1 of the PIPA, in general, the employer shall also comply with the same rules as those for the cross-border transfer of non-sensitive personal information.





Taiwan

In Detail

In addition, according to Article 21 of the PIPA, when an employer transfers employee personal data internationally, the central competent authority may apply restrictions in any of the following circumstances:

- (1) where substantial interests of the nation are involved;
- (2) where required by international treaties or agreements;
- (3) where the country to which the personal data are transferred does not have robust laws and regulations to protect personal data, leading to prospective infringement of the employees' rights; or
- (4) where the employees' personal data are transferred to a third country or region to circumvent the application of the PIPA.

6. What are the legal restrictions on transferring employees' personal data to a third party?

If the employer intends to transfer the non-sensitive personal information of employees to a third party for use by such third party, unless the circumstances listed in our response to question 3A(B) are met, the employees shall be notified, pursuant to Article 8 of the PIPA, with respect to which entity will be using such personal information. In addition, the act of providing employee personal information to a third party for the third party's use must still be within the scope of necessity for the specific purpose that the employer is collecting such information.

As for sensitive personal information, following the response to question 3, such information may only be collected, processed or used if the circumstances under Article 6, Paragraph 1 of the PIPA are met. If an employer meets such requirements and intends to transfer such information to a third party, in addition to the requirements under Article 6, Paragraph 1 of the PIPA, in general, the employer shall also comply with the same rules as those for the transfer of non-sensitive personal information to a third party.

If the third party is outside of the country, the transfer is accordingly both to a "third party" and "cross-border" in nature, thus the employer must also follow the aforementioned rules on transferring personal information outside of the country.





Taiwan

In Detail

7. What are the consequences of breaching privacy laws in your jurisdiction?

An employer that violates the provisions of the PIPA may be subject to civil, criminal and/or administrative liabilities.

Civil liabilities

The PIPA provides that employees may claim damages against an employer if it has violated the legislation. A foundation or a nonprofit organization may also file a class action on behalf of employees whose privacy rights are violated by their employer.

Criminal liabilities

The penalties for such violations are imprisonment for not more than five years, detention and/or a fine of not more than TWD 1 million. Further, a prosecutor may initiate investigations for the crimes provided under the PIPA without an employee's or victim's complaint.

Administrative liabilities

For certain violations of the PIPA, where an employer does not rectify the violations within the time limit notified by the competent authority, depending on the particular violation of the PIPA, the employer will be fined an amount ranging from TWD 50,000 to TWD 500,000 or TWD 20,000 to TWD 200,000 for each repeated violation and for every continuing violation. The employer's representative, manager or other person who may represent the employer may also be fined the same amount, except for the latter, who may prove that he/she has performed his/her duty to prevent such violation.

8. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee's personal data?

There is no current response plan in Taiwan with respect to the EU's implementation of the General Data Protection Regulation ("GDPR") on May 25, 2018. Employers should nevertheless pay close attention to the implementation of the GDPR, as well as to whether amendments are made to the PIPA or other relevant regulations in response.

Contributed by: **Chung-Teh Lee & Elizabeth Pai**, Lee, Tsai & Partners, Attorneys-at-Law

[HOME](#)[COUNTRIES](#)[DIRECTORY](#)

August 2018

SCROLL DOWN



Thailand



Contributed by: Tilleke & Gibbins



In Brief



In Detail

Contributed by: David Duncan, Tilleke & Gibbins



[Link to biography >](#)



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



Thailand

In Brief

1. Is there a law regulating applicant personal data?

The law does not specifically address an employer's handling of personal data of prospective employees, but general provisions of law are applicable.

2. Is there a law regulating employee personal data?

The law does not specifically address an employer's handling of personal data of its employees, but general provisions of law are applicable.

3. Do I need to have a privacy statement or agreement?

No, but it is advisable to obtain consent, so as to reduce the employer's risks under general provisions of law.

4. How long must I retain employee data? What is best practice?

An employee register must be maintained during employment and for a period of two years after the end of the employment relationship. Pay documentation must be maintained for two years after payment. Both the employee register and pay documentation would need to be maintained for longer in the event of certain complaints and/or litigation. In addition, separate requirements apply in relation to identification information and computer traffic data under the Computer Crimes Act. The statute of limitations for claims for unfair termination is ten years. Hence, it would be advisable for an employer to retain information in line with these periods.

5. Can I transfer employee data overseas?

The law does not specifically address transfer of employee data overseas, but general provisions of law are applicable.

6. Can I transfer employee data to a third party?

The law does not specifically address transfer of employee data to third parties, but general provisions of law are applicable.

7. What are the consequences of breach?

Depending on the particulars of the breach, possible consequences could include an award of damages, an order to take remedial action, fines and/or imprisonment.

8. What are the main pitfalls?

It would be advisable for employers to keep in mind that they may have data retention obligations under the Computer Crimes Act.





Thailand

In Detail

1. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant’s personal data in your jurisdiction?

The law does not specifically address an employer’s handling of personal data of prospective employees. However, general provisions of law would be applicable. For example, in the case of unauthorized disclosure of personal data that causes damage, the person suffering damage could bring a civil claim for defamation. Further, a criminal complaint of defamation would also be possible in some circumstances.

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee’s personal data in your jurisdiction?

Pursuant to the Labor Protection Act, an employer is required to maintain an employee register containing at least the following:

- name and family name;
- sex;
- nationality;
- date of birth or age;
- current address;
- date of commencement of employment;
- position or duty;
- wages or other remuneration that the employer agrees to pay to the employee; and
- date of termination of employment.





Thailand

In Detail

An employer with ten or more employees must prepare documents concerning the payment of wages, overtime pay, holiday pay, and holiday overtime pay, which must contain at least the following:

- working days and working hours;
- work performed by the employee who receives wages on a work-unit basis; and
- rates and amount of wages, overtime pay, holiday pay, and holiday overtime pay that each employee shall receive.

Employers must require employees to sign such documents. Where remuneration is paid by electronic transfer, evidence of the transfer is deemed to be a document relating to such payment.

Aside from the foregoing, the law does not specifically address an employer's handling of employee personal data. Nevertheless, similar to the position in respect of prospective employees, general provisions of law are applicable. For example, in the case of unauthorized disclosure of personal data that causes damage, a person suffering damage could bring a claim for civil defamation. Further, a criminal complaint of defamation would also be possible in some circumstances.

3. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee's personal data?

No, but it would be advisable to obtain consent, so as to reduce the employer's exposure under general provisions of law, in the case of unauthorized disclosure.

4. For how long must an employer retain an employee's personal data? What is best practice?

An employer must maintain the employee register for at least two years from the date of termination of employment of each employee, and the employer must keep documents relating to payment of remuneration for at least two years from the date of payment thereof. However, if a complaint has been submitted under the Labor Protection Act, if there is a dispute under the Labor Relations Act, or if there is litigation involving employment, the employer must keep the employee register and documents relating to the payment of remuneration until the issuance of a final order or judgment concerning the matter.





Thailand

In Detail

Please also see response to question 8 below, which addresses the maintenance of identification information and computer traffic data under the Computer Crimes Act.

Aside from the foregoing, it should be noted that the statute of limitations for claims for unfair termination is ten years from when the claim could be brought (subject to interruption as provided in statute). Hence, it would be advisable to retain all information until the relevant periods lapse.

5. What are the legal restrictions on transferring employees' personal data outside your jurisdiction?

The law does not specifically address transfer of employee information to recipients outside Thailand. However, please see comments in response to question 2 above, on the application of general provisions of law. Such comments would be equally applicable in response to this question.

6. What are the legal restrictions on transferring employees' personal data to a third party?

The law does not specifically address transfer of employee information to third parties, whether in Thailand or abroad. However, please see comments in response to question 2 above, on the application of general provisions of law. Such comments would be equally applicable in response to this question.

7. What are the consequences of breaching privacy laws in your jurisdiction?

A comprehensive Personal Data Protection Bill has been pending (in various forms) for some years but, at present, Thailand lacks a comprehensive personal data protection regime. Nevertheless, as noted, general provisions of law are applicable. For example, in the case of unauthorized disclosure of personal data that causes damage, a person suffering damage could bring a civil claim for defamation. In that situation, the consequences could be an award of damages and/or an order to take remedial action. Further, in a case of a criminal complaint of defamation, the Criminal Code specifies penalties including imprisonment up to one year and/or a fine of up to THB 20,000, as well as the possibility that the court may order remedial action. As for a defamation offense under the Computer Crimes Act, penalties include imprisonment up to three years and a fine of up to THB 200,000.





Thailand

In Detail

8. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee’s personal data?

Employers should keep in mind that they may have data retention obligations under the Computer Crimes Act. Where an employer provides internet access or certain other IT services for use by its employees, the employer would be regarded as a service provider under the Act. A service provider must store user identification data such that the service user can be identified from the beginning of use of the service, and the service provider must keep this data for at least 90 days after termination of the service. In addition, a service provider must:

- store traffic data, the specifics of which depend on the type of service provider and the type of service(s) being provided; and
- maintain that traffic data for 90 days (or longer if so requested by a competent official, but not to exceed one year).

The regulations also require a service provider to put in place a system that meets specified requirements in terms of security and reliability.

Contributed by: **David Duncan**, Tilleke & Gibbins



[Link to biography >](#)



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 



Vietnam



Contributed by: **Mayer Brown (Vietnam) LLC**



In Brief



In Detail

Contributed by: **Hoang Anh Nguyen & Huong Nguyen, Mayer Brown (Vietnam) LLC**



[Link to biography >](#)



[Link to biography >](#)



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN



Vietnam

In Brief

1. Is there a law regulating applicant personal data?

Yes. There are a number of laws regulating applicant personal data, specifically:

- The Labor Code No. 10/2012/QH13 (“**Labor Code**”); and
- The Civil Code No. 91/2015/QH13 (“**Civil Code**”).

2. Is there a law regulating employee personal data?

There is no single comprehensive law or code on employee personal data in Vietnam. In some specific circumstances, however, the Civil Code, Penal Code, Information Technology Law and Cyber Information Security Law are applicable to protect data privacy.

3. Do I need to have a privacy statement or agreement?

No, there is no legal requirement to have a privacy statement or agreement to deal with employee personal data in Vietnam.

4. How long must I retain employee data? What is best practice?

There is no statutory requirement regarding the retention of employee data. In practice, an employer should agree with an employee on the time limit for retaining his/her data. It is best practice to obtain written consent from the employee.

5. Can I transfer employee data overseas?

Yes, subject to Article 38 of the Civil Code, which provides that the collection and publication of personal data pertaining to a person must be subject to his/her consent.

6. Can I transfer employee data to a third party?

Yes, subject to Article 38 of the Civil Code, which provides that the collection and publication of personal data pertaining to a person must be subject to his/her consent.

7. What are the consequences of breach?

An employee could sue the breaching party for compensation if the employee has suffered damage to his/her health, honor, dignity or reputation. The employer could also potentially be subject to an administrative penalty.

8. What are the main pitfalls?

The main pitfall is the compensation that may be payable by an employer to an employee for breaching data privacy laws.





Vietnam

In Detail

1. Is there a law/Code or other similar document regulating the collection, use and/or handling of an applicant’s personal data in your jurisdiction?

The laws regulating applicant personal data include:

- The Labor Code No. 10/2012/QH13 dated June 18, 2012 of the National Assembly (“**Labor Code**”); and
- The Civil Code No. 91/2015/QH13 dated November 24, 2015 of the National Assembly (“**Civil Code**”).

Although the laws protect the right to privacy by requiring prior consent for gathering private information, there is no definition under current Vietnamese law that defines the “privacy” or “personal information” of an individual. Under the current regulations specific to certain sectors, “personal information” is generally defined to mean information sufficient to identify an individual which includes, among other things, name, date of birth, profession, title, address, email address, telephone number, identification card number, passport number, medical records, tax record, social insurance card number and credit/debit card number. The interpretation of whether or not information is considered to be personal would be at the sole discretion of the state agency in question.

As a matter of Vietnamese law, before entering into a labor contract, employers are permitted to require applicants to provide them with information regarding name, sex, residency, education background, professional qualifications, health status and other information directly relating to the signing of the labor contract.

2. Is there a law/Code or other similar document regulating the collection, use and/or handling of an employee’s personal data in your jurisdiction?

There is no single comprehensive law or code on employee personal data in Vietnam. In some specific circumstances, however, the Civil Code, Penal Code, Information Technology Law and Cyber Information Security Law are applicable to protect data privacy.

The laws apply to a large number of organizations and individuals. All organizations and individuals have a duty to respect private and confidential information. The disclosure of protected information is, however, possible where:

- (a) it is specifically permitted by the laws;





Vietnam

In Detail

- (b) the information owner has provided his/her prior consent to such intended disclosure; or
- (c) it is at the request or on the order of any state competent agency (for example, as ordered by a competent court).

Specifically, pursuant to Article 38 of the Civil Code, the privacy of an individual is protected by law. The collection and publication of information and data pertaining to an individual shall be subject to his/her consent. Exceptions apply in relation to the collection and publication of personal information as referred to in (a) and (b) above.

An employer must take measures to protect the personal information provided by an employee. It must ensure that the information shall be used only for the purpose of the employment relationship. The use of the information for any other purpose or by any third party shall be subject to the employee's prior consent.

3. Is there a legal requirement to have a document (e.g., privacy policy, personal information collection statement, agreement) to deal with an employee's personal data?

There is no statutory requirement regarding having a privacy policy or an agreement relating to employee personal information. In practice, an employer should agree with the employee on how it will deal with his/her personal data. It would be preferable for the employer to obtain the employee's written consent.

4. For how long must an employer retain an employee's personal data? What is best practice?

The Labor Code does not provide any regulations on the retention of an employee's personal data. The sole provision on the term of retaining an employee's personal data, contained in Circular No. 09/2011/TT-BNV dated June 3, 2011, stipulates that the term of retaining a seasonal employment contract (for a seasonal or specific job that has a duration of under 12 months) of an employee will be five years from the date of termination (number 66 in the table of preservation term of records and materials generally formed in activities of agencies and organizations issued together with this Circular).

In practice, an employer should agree with an employee on the time limit for retaining his/her data. It is best practice to obtain the employee's written consent. Employers in Vietnam will generally retain their employees' data for as long as they can.





Vietnam

In Detail

5. What are the legal restrictions on transferring employees' personal data outside your jurisdiction?

Article 38 of the Civil Code provides that the collection and publication of personal data pertaining to a person must be subject to his/her consent. An employer, therefore, should obtain an employee's written consent before transferring his/her data outside the jurisdiction.

6. What are the legal restrictions on transferring employees' personal data to a third party?

As above, Article 38 of the Civil Code provides that the collection and publication of personal data pertaining to a person must be subject to his/her consent. Consent should therefore be obtained from the employee before the employer transfers employee personal data to a third party.

7. What are the consequences of breaching privacy laws in your jurisdiction?

The employee could sue the breaching party in a court for compensation if the employee has suffered damage to his/her health, honor, dignity or reputation. Depending upon the seriousness of the breach, the employer could be subject to an administrative penalty.

8. What are the main pitfalls or areas to watch out for in your jurisdiction regarding the collection, use and/or handling of an employee's personal data?

Vietnamese law protects rights related to private information, state secrets, trade secrets, and credit information. All organizations and individuals have a duty to respect private and confidential information. Any breach of this confidentiality obligation would, depending on the seriousness of the breach, result in an administrative penalty or a criminal sanction. However, the main pitfall is the compensation that may be payable by an employer to an employee for breaching data privacy laws. The value of compensation varies on a case-by-case basis.

Contributed by: **Hoang Anh Nguyen & Huong Nguyen**, Mayer Brown (Vietnam) LLC



[Link to biography >](#)



[Link to biography >](#)



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 

Directory

 Australia



John Tuck

Corrs Chambers Westgarth,
567 Collins Street, Melbourne, VIC 3000, Australia



+61 3 9672 3000



john.tuck@corrs.com.au



www.corrs.com.au/people/john-tuck/

 Australia



Anthony Forsyth

Corrs Chambers Westgarth,
567 Collins Street, Melbourne, VIC 3000, Australia



+61 3 9672 3000



anthony.forsyth@corrs.com.au



www.corrs.com.au/people/anthony-forsyth/

 Hong Kong



Duncan Abate

Mayer Brown,
16th - 19th Floors, Prince's Building, 10 Chater Road, Central, Hong Kong



+852 2843 2203



duncan.abate@mayerbrown.com



www.mayerbrown.com/people/duncan-a-w-abate/



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 

Directory

 Hong Kong



Hong Tran

Mayer Brown,
16th - 19th Floors, Prince's Building, 10 Chater Road, Central, Hong Kong



+852 2843 4233



hong.tran@mayerbrown.com



www.mayerbrown.com/people/hong-tran/

 India



Ajay Raghavan

Trilegal,
The Residency, 7th Floor, 133/1, Residency Road, Bangalore 560 025, India



+91 80 4343 4646



ajay.raghavan@trilegal.com



www.trilegal.com/index.php/member-profile/ajay-raghavan

 India



Swarnima

Trilegal,
The Residency, 7th Floor, 133/1, Residency Road, Bangalore 560 025, India



+91 80 4343 4646



swarnima@trilegal.com



<https://www.trilegal.com/index.php/member-profile/Swarnima->



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 

Directory

Indonesia



Fahrul S. Yusuf

SSEK Indonesian Legal Consultants,
14th Floor Mayapada Tower, Jl. Jend. Sudirman Kav. 28, Jakarta 12920, Indonesia



+62 21 521 2038



fahrulyusuf@ssek.com



<https://www.ssek.com/attorneys/partners/fahrul-s-yusuf>

Japan



Nobuhito Sawasaki

Anderson Mori & Tomotsune,
Otemachi Park Building, 1-1-1 Otemachi, Chiyoda-ku, Tokyo 100-8136, Japan



+81 3 6775 1087



nobuhito.sawasaki@amt-law.com



www.amt-law.com/en/professional/profile/ns

Macau



Tiago Vilhena

MdME Lawyers,
Avenida da Praia Grande, 409 China Law Building, 21/F and 23/F A-B, Macau



+853 2833 3332



tv@mdme.com.mo



mdme.com.mo/main/corporate/tiago-vilhena



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 

Directory

Macau

António Tam

MdME Lawyers,
Avenida da Praia Grande, 409 China Law Building, 21/F and 23/F A-B, Macau

 [+853 2833 3332](tel:+85328333332)  cntam@mdme.com.mo

 mdme.com.mo/main/insurance/antonio-tam

Malaysia

Wong Kian Jun

Shearn Delamore & Co.,
7th Floor, Wisma Hamzah-Kwong Hing, No.1 Leboh Ampang, 50100 Kuala Lumpur, Malaysia

 [+603 2027 2727](tel:+60320272727)  wongkj@shearndelamore.com

 www.shearndelamore.com/people/wong-kian-jun/

Myanmar

Chester Toh

Rajah & Tann NK Legal Myanmar Company Limited,
Myanmar Centre Tower 1, Floor 07, Unit 08, 192 Kaba Aye Pagoda Road, Bahan Township, Yangon, Myanmar

 [+959 7304 0763](tel:+95973040763)  chester.toh@rajahtann.com

 www.rajahtannasia.com/chester.toh



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 

Directory

 Myanmar**Lester Chua**

Rajah & Tann NK Legal Myanmar Company Limited,
Myanmar Centre Tower 1, Floor 07, Unit 08, 192 Kaba Aye Pagoda Road, Bahan Township, Yangon, Myanmar



+959 7304 0763



lester.chua@rajahtann.com



<https://www.rajahtannasia.com/lester.chua>

 New Zealand**Carl Blake**

Simpson Grierson,
Level 27, Lumley Centre, 88 Shortland Street, Auckland 1010, New Zealand



+64 9 977 5233



carl.blake@simpsongrierson.com



www.simpsongrierson.com/people/carl-blake

 Pakistan**Zeeshan Ashraf Meer**

Meer & Hasan,
306 Al-Faisal Plaza, 48 The Mall Road, Lahore 54000, Pakistan



+92 42 3723 5812



mail@meerhasan.com



www.meerhasan.com/index.php/index.php?option=com_content&view=article&id=138&Itemid=533



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 

Directory

 PRC



Deng Youping

Jingtian & Gongcheng,
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China



+86 10 5809 1033



deng.youping@jingtian.com



www.jingtian.com/eng/node/241

 PRC



Andy Yeo

Mayer Brown,
Suite 4710, Tower I, Plaza 66, 1266 Nan Jing Road West, Shanghai 200040, China



+86 21 6032 0266



andy.yeo@mayerbrown.com



www.mayerbrown.com/people/andy-s-yeo

 Philippines



Enriquito J. Mendoza

Romulo Mabanta Buenaventura Sayoc & de los Angeles,
21st Floor, Philamlife Tower, 8767 Paseo De Roxas, Makati City 1226, Philippines



+63 2 555 9555



enriquito.mendoza@romulo.com



www.romulo.com/mendoza-enriquito-j/



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 

Directory

 Singapore



Kala Anandarajah
Rajah & Tann Singapore LLP,
9 Battery Road, #25-01 Straits Trading Building, Singapore 049910

 [+65 6 535 3600](tel:+6565353600)  kala.anandarajah@rajahtann.com

 www.rajahtannasia.com/one-team/partners/kala-anandarajah-pbm

 South Korea



Michael Kim
Kim & Chang,
39, Sajik-ro 8-gil, Jongno-gu, Seoul 03170, Korea

 [+82 2 3703 1114](tel:+82237031114)  michael.kim@kimchang.com

 www.kimchang.com/frame2.jsp?lang=2&b_id=87&mode=view&idx=1881

 South Korea



Joo Hee Kim
Kim & Chang,
39, Sajik-ro 8-gil, Jongno-gu, Seoul 03170, Korea

 [+82 2 3703 1114](tel:+82237031114)  joohee.kim@kimchang.com

 www.kimchang.com/frame2.jsp?lang=2&b_id=87&mode=view&idx=1850



Directory

 South Korea

Ari Yoon

Kim & Chang,
39, Sajik-ro 8-gil, Jongno-gu, Seoul 03170, Korea



[+82 2 3703 1114](tel:+82237031114)



ari.yoon@kimchang.com



www.kimchang.com/frame2.jsp?lang=2&b_id=87&mode=view&idx=2168

 Sri Lanka

John Wilson

John Wilson Partners,
365 Dam Street, Colombo 12, Sri Lanka



[+94 11 2324579](tel:+94112324579)



advice@srilankalaw.com



www.srilankalaw.com/people/

 Taiwan

Chung-Teh Lee

Lee, Tsai & Partners, Attorneys-at-Law,
9F, 218 Tun Hwa S. Road, Sec. 2, Taipei 106, Taiwan



[+886 02 2378 5780](tel:+886223785780)



ctlee@leetsai.com



www.leetsai.com/portfolio-item/dr-chung-teh-lee



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 

Directory

 Taiwan



Elizabeth Pai

Lee, Tsai & Partners, Attorneys-at-Law,
9F, 218 Tun Hwa S. Road, Sec. 2, Taipei 106, Taiwan



+886 02 2378 5780



elizabethpai@leetsai.com



www.leetsai.com/portfolio-item/elizabeth-pai

 Thailand



David Duncan

Tilleke & Gibbins,
Supalai Grand Tower, 26th Floor, 1011 Rama 3 Road, Chongnonsi, Yannawa, Bangkok 10120, Thailand



+66 2056 5555



david.d@tilleke.com



www.tilleke.com/index.php?q=professionals/david-duncan

 Vietnam



Hoang Anh Nguyen

Mayer Brown (Vietnam) LLC,
Suite 606, 6th Floor, Central Building, 31 Hai Ba Trung, Hoan Kiem District, Hanoi, Vietnam



+84 4 3266 3113



hoanganh.nguyen@mayerbrown.com



<https://www.mayerbrown.com/people/hoang-anh-nguyen/>



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 

Directory

 Vietnam



Huong Nguyen

Mayer Brown (Vietnam) LLC,
Suite 606, 6th Floor, Central Building, 31 Hai Ba Trung, Hoan Kiem District, Hanoi, Vietnam



+84 4 3266 3113



huong.nguyen@mayerbrown.com



<https://www.mayerbrown.com/people/huong-thi-nguyen/>



HOME



COUNTRIES



DIRECTORY

August 2018

SCROLL DOWN 

Legal Statement

This publication provides information and comments on legal issues and developments of interest to our clients and friends. The foregoing is not a comprehensive treatment of the subject matter covered and is not intended to provide legal advice. Readers should seek legal advice before taking any action with respect to the matters discussed herein.

© 2018 Mayer Brown. All rights reserved.

Attorney advertising. Prior results do not guarantee a similar outcome.



HOME



COUNTRIES



DIRECTORY

August 2018