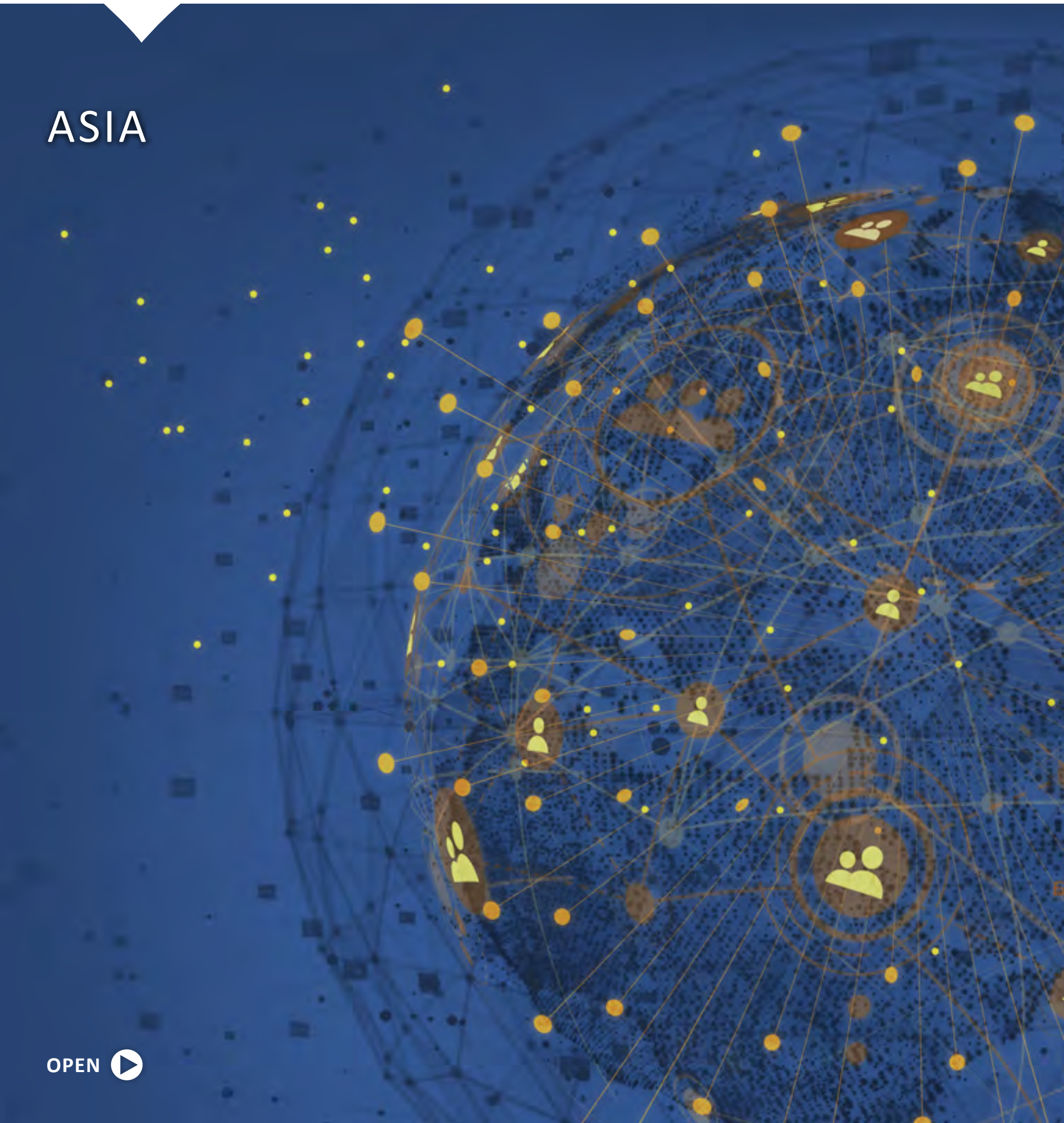
A Regional Guide to Employee Data Privacy

ASIA



OPEN

Introduction

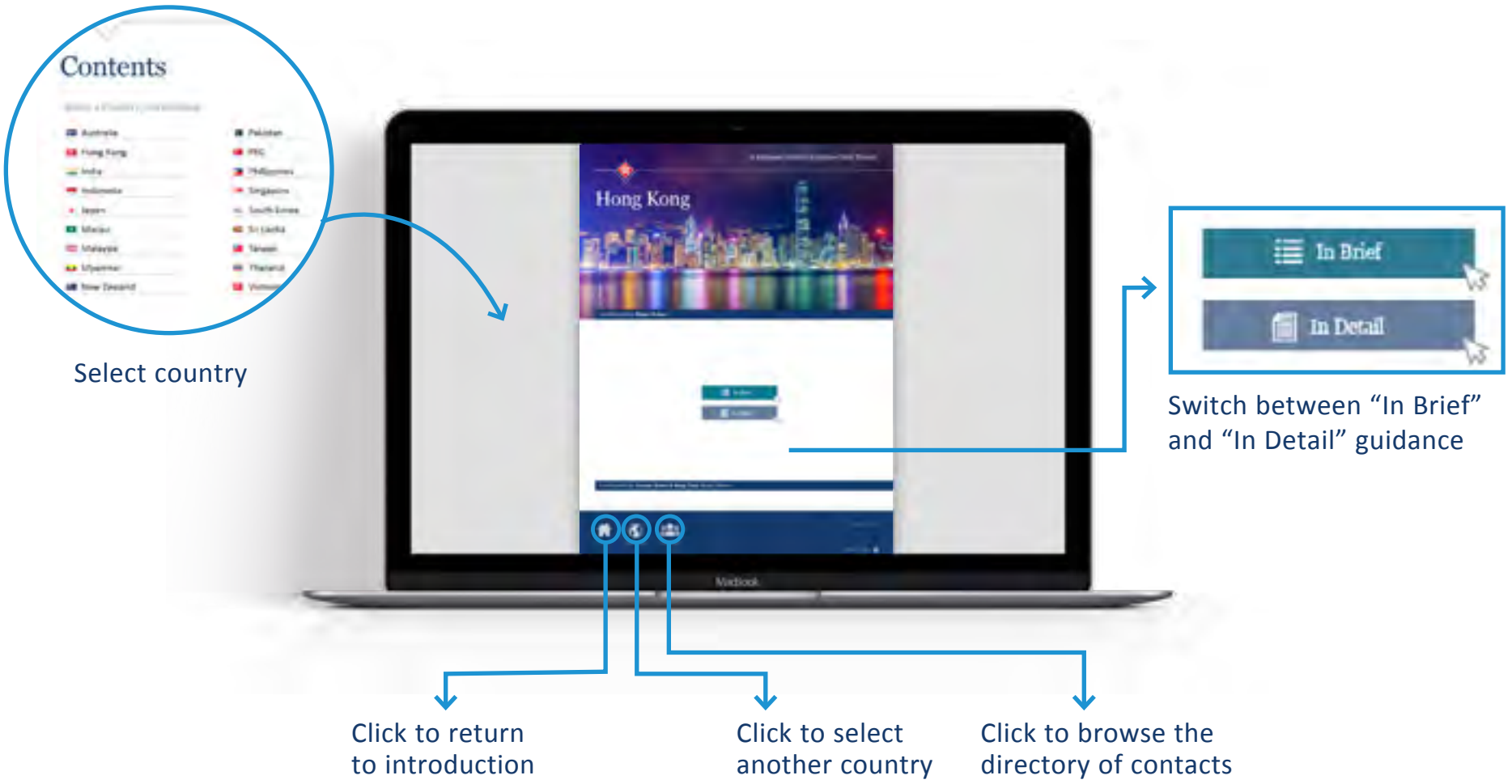
Data privacy is a priority for all employers but especially those with operations in more than one country. It impacts all aspects of the employment relationship and, with the increase in data transfers between businesses and across borders, employers often need to comply with multiple laws to minimize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



Select country

Switch between “In Brief” and “In Detail” guidance

Click to return to introduction

Click to select another country

Click to browse the directory of contacts

Japan

Contributed by: **Anderson Mori & Tomotsune**

ANDERSON MŌRI & TOMOTSUNE

In Brief

In Detail

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

Link to biography >

Japan

ANDERSON MŌRI & TOMOTSUNE

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

ANDERSON MŌRI & TOMOTSUNE

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

ANDERSON MŌRI & TOMOTSUNE

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

ANDERSON MŌRI & TOMOTSUNE

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

ANDERSON MŌRI & TOMOTSUNE

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 >

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

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.