# Comparative guide on data protection across Asia-Pacific

July 2022

# Table of Contents

# China

## General questions

**1. What is the applicable legislation governing data protection in your jurisdiction, for both personal information and non-personal information?**

The Cyber Security Law ("**CSL**") (effective from 1 June 2017), provides some general legislation on data protection, including data localisation for critical information infrastructure operators and general requirements on data protection (including personal information). The CSL does not provide comprehensive rules on data protection, however, as it is a consolidated law for cyber security protection.

The Data Security Law ("**DSL**") came into effect on 1 September 2021. The DSL is the consolidated law in China on data protection and applies generally to data processing activities in China. The Personal Information Protection Law ("**PIPL**"), which came into effect on 1 November 2021, focuses on the protection of personal information.

On 14 November 2021, China's watchdog on data protection, the Cyberspace Administration of China ("**CAC**"), issued the draft *Network Data Security Administration Regulations*. These regulations implement the rules of the DSL and PIPL and regulate both personal and non-personal information. The CAC has also released measures on the cross-border transfer of personal information.

**2. Who is/ are the regulator(s) in your jurisdiction for data protection?**

- the Cyberspace Administration of China, who focus on data protection (including personal information, important data, cross-border transfer of data), cyber security review, etc.
- the Ministry of Industry and Information Technology, who focus on the safety of industrial data and telecommunication data. They also regulate apps' compliance with the protection of personal information.
- the Ministry of Public Security, who focus on cyber security incidents, data security incidents, and combatting against data security or cyber security crimes.
- Sector regulators, who focus on sector-specific data protection and important data identification.

### 3. Who is governed by the data protection legislation in your jurisdiction?

The DSL regulates data processing activities carried out within the territory of China. Therefore, persons or entities carrying out data processing activities are subject to the regulation of the DSL. The DSL further provides that data processing activities involving personal information shall also comply with the relevant laws and regulations.

The PIPL applies to the processing activities of personal information which occur within the territory of China. The PIPL also has an extra-territorial application clause. Under this clause, the PIPL also applies to offshore personal information processing of natural persons in China which is processed for the purpose of providing services or products to natural persons in China, or analysing or evaluating the behaviour of natural persons in China.

### 4. Is there an extraterritorial application effect under the data protection legislation in your jurisdiction?

As stated in question 3, the PIPL has a provision which provides an extra-territorial application effect. This means the PIPL also applies to foreign personal information processing activity if it meets the requirements under this provision, i.e. processing personal information of natural persons in China for the purpose of providing services or products to natural persons in China, or analysing or evaluating the behaviour of natural persons in China.

The DSL, on the other hand, has a provision which provides for a very limited extra-territorial application effect. Article 2, paragraph 2 of the DSL provides that if offshore data processing activities damage the national security and public interest of China, or the legitimate rights and interests of citizens or organisations in China, accountability and liability will be pursued in accordance with the law.

### 5. What are the key aspects to look for when processing personal information in your jurisdiction?

- **Processing with lawful basis**—as prescribed under Article 13 of the PIPL, the processing of personal information shall have a lawful basis. This includes obtaining the data subject's consent, the necessity for conclusion or performance of contracts with data subjects, the necessity for human resource management, statutory obligations, necessity for responding to public health emergencies or emergency situations, public interest in case of news reporting, public opinion monitoring, and processing personal information that is already in the public domain.
- **Separate consent**— the PIPL requires data processors to obtain the data subject's separate consent for certain types of data processing activities. This includes the processing of sensitive personal information, cross-border transfer of personal information, sharing data to another data handler (i.e. the persons/entities decide the purpose and method for the processing of data and/or personal information), and disclosing personal information to the public.
- **Transparency**—the PIPL provides that the data handler shall, before processing PI, inform individuals of relevant information about the data processing, including the names and contact information of the data handler; processing purposes; method of processing; categories of PI processed, and the retention period; and methods and procedures for individuals to exercise their rights, etc.
- **Data subject's rights**—under the PIPL data subjects have the right to request the data handler to access, copy as well as to correct or supplement his/her personal information. Data subjects also have the right to withdraw their consent to the processing of their personal information.

— **Channel options for cross-border transfer of personal information**—to transfer personal information out of China, the data handler must fulfil one of the three channel options for cross-border transfer—undergo the regulator's security assessment, obtain certification by a third-party institution, or sign the standard contractual clauses ("**SCCs**") with the foreign data recipients. The CAC has released measures on the three channel options, which provides more detailed rules for implementation.

### 6. What are the key aspects to look for when processing non-personal information in your jurisdiction?

Article 21 of the DSL prescribes that the state shall establish a mechanism to protect data based on the categories and grading of the data. Important data is subject to enhanced protection. The key aspects to look for are:

— **Data Classification**: the persons/entities shall classify data into different categories and grades, and will manage the data based on its categories and grades. Some sector regulators have released their guidelines for data classification in their respective sectors, such as the industrial sector, and the stocks and futures sectors.

— **Important data identification and protection**— The DSL provides that regulators in each sector or region shall formulate and publish the catalogue of important data in their respective sector or region. Entities processing data in China must consider the relevant catalogue in their sector/region. The DSL imposes further rules on persons/entities processing important data, including data localisation requirements, carrying out regular risk assessments, and appointing a data protection officer in accordance with further rules to be implemented by the CAC. In November 2021, the CAC issued the draft Network Data Security Administration Regulations, which provide more comprehensive obligations for the processing of important data.

### 7. Is there a requirement for data localisation in your jurisdiction?

Yes. According to article 37 of the Cybersecurity Law, critical information infrastructure operators ("**CIIOs**") shall store personal information and important data collected and generated during their operations in China within the territory of China. If the CIIO needs to transfer the data out of China for business needs, it shall undergo a security assessment as formulated by the CAC.

Article 40 of the PIPL stipulates that the CIIOs and large-scale operators, i.e. data handlers that meet the threshold requirement to be formulated by the CAC, shall store the personal information collected and generated in China within the territory of China. If the data handler needs to transfer the data out of China, it shall undergo the security assessment by the CAC.

The DSL provides that the cross-border transfer of important data collected and generated in China by non-CIIOs shall comply with the relevant measures to be formulated by the CAC.

On 7 July 2022, the CAC issued the *Measures on Security Assessment for Cross-border Transfer of Data* ("**Security Assessment Measures**"), which will come into force on 1 September 2022. The Security Assessment Measures provide the scope of cross-border data transfer activities that shall undergo a security assessment before the transfer of data.

Under the Security Assessment Measures, the following types of cross-border data transfer shall not be carried out without first obtaining the approval of the CAC after its security assessment:

- Cross-border transfer of important data;
- Cross-border transfer of personal information by CIIOs or data handlers that processes more than 1,000,000 natural persons' personal information;
- Cross-border transfer of personal information by data handers that from 1 January of the previous year accumulatively transfer more than 100,000 natural persons' personal information or more than 10,000 natural persons' sensitive personal information out of China.

According to the Security Assessment Measures, cross-border data transfer activities carried out before the effective date of the Security Assessment Measures, shall complete the rectification to follow the requirements of the Security Assessment Measures within six months after it takes force.

### 8. What are the requirements for cross-border transfer of data in your jurisdiction?

For cross-border transfer of personal information that does not fall under the scope that is subject to the security assessment, the data handler shall:

a. Obtain the separate consent of the data subjects;
b. Conduct the protection impact assessment before the transfer;
c. Satisfy one of the channel options for cross-border transfer of personal information described under question 5.

For non-personal data, if the cross-border transfer involves important data, it must also undergo the security assessment.

# Questions specific to the life sciences & healthcare sector

### 9. From the perspective of personal information protection, during the clinical trial of a pharmaceutical/medical device/other types of healthcare products, how is the clinical trial data regulated? Do the general requirements in the questions above apply, or is clinical trial data regulated differently? If it is regulated differently, how is it regulated?

Under Chinese law, clinical trial data refers to the data generated during clinical trials of pharmaceutical/medical device/other types of healthcare products that are primarily used for marketing approval registrations. There are no regulations specifically governing clinical trial data in China. This type of data is mainly managed as one of the elements of clinical trials contained in quality management codes, such as the *Good Clinical Practice for Clinical Trials of Drugs and Good Clinical Practice for Clinical Trials of Medical Devices* (the "GCPs").The GCPs have specific requirements for the collection, recording, access and preservation of clinical trial data, but their main purpose is to ensure that the data used for pharmaceutical/medical device/other types of healthcare products registration applications are true, scientific, adequate and reliable, and therefore do not distinguish between "personal information" and "non-personal information". Nonetheless, the GCPs contain specific requirements for the protection of the privacy of subjects and their information, which shall be followed by the parties involved in the clinical trials.

The requirements of the GCPs include, but are not limited to:

- Sponsors should use a “subject identification code”, which is a unique code assigned to a subject in a clinical trial to identify him or her. This code is used by the investigator in place of the subject's name to protect their privacy when reporting adverse events and other data relating to the trial.
- Sponsors should inform data subjects in the informed consent form relating to the clinical trial (and other information provided to the data subject) that, subject to the principle of confidentiality and the relevant regulations, supervisors, inspectors, ethics committees and drug regulatory authority inspectors may have access to the subject's original medical records to verify the course and data of the clinical trial.
- In cases such as the continued storage of remaining specimens after the end of a clinical trial or their possible future use, an informed consent from should be signed by the subject. The form should give details of the duration of storage and the confidentiality of the data, as well as the circumstances under which the data and specimens can be shared with other investigators, etc.

Based on the above, during the clinical trial of a pharmaceutical/medical device/other types of healthcare products, when the data related to the clinical trial involves personal information, the relevant entity should firstly comply with the requirements of the general personal information protection regulations. On this basis, it should also comply with the relevant provisions of the GCPs regarding the protection of privacy.

**10. From the perspective of personal information protection, after the pharmaceutical/medical device/other types of healthcare products is marketed, how is the post-marketing data (for example, pharmacovigilance data) regulated? Do the general requirements in the questions above apply? If it is regulated differently, how is it regulated?**

There are various types of post-marketing data for pharmaceutical/medical device/other types of healthcare products, one of which is pharmacovigilance data. This is the main category of data related to personal information and is especially relevant with regards to data from individual adverse drug reaction reports.

According to the *Good Practice for Pharmacovigilance*, a valid individual adverse drug reaction report should include information on the identifiable patient, the identifiable reporter, the suspected drug, and a description of the adverse reaction. This dictates that personal information such as the name or initials, sex, age, and illness of the patient concerned will be collected, stored, and used. Chinese law does not have a separate regulation for the type of personal information involved in the pharmacovigilance process. Therefore, the general personal information protection regulations will apply when pharmacovigilance data involves personal information. In addition, when regulations such as the Drug Administration Law and the *Good Practice for Pharmacovigilance* (which relate to the protection of personal information), conflict with the general personal information protection regulations, the laws relating to pharmacovigilance shall prevail.

Specifically, under the *Drug Administration Law*, the collection and reporting of adverse drug reactions is a statutory obligation of the holder of a pharmaceutical marketing authorization, pharmaceutical manufacturers, pharmaceutical distributors, and medical institutions. As a result, some of the rights of patients as subjects of personal information under the PIPL may be limited by the statutory obligation of pharmacovigilance. Where a patient's rights under the PIPL conflict with the statutory obligation to collect pharmacovigilance data, the fulfilment of the statutory obligation to collect pharmacovigilance data shall take precedence.

For example, Article 13(1) (iii) of the PIPL provides that "the holder of personal information may handle personal information only if one of the following circumstances is met: ... (iii) it is necessary for the performance of statutory duties or legal obligations ...". In other words, carrying out pharmacovigilance activities and the processing of patients' personal information during the collection and reporting of adverse drug reactions is part of the fulfilment of the data collector's legal obligations. It does not therefore require the consent of the patient.

Another example is the *Good Practice for Pharmacovigilance*, which requires that pharmacovigilance records and data are kept until at least ten years after the cancellation of the drug registration certificate. Therefore, the patient cannot request the holder to delete personal information under the PIPL until the expiry of the pharmacovigilance data retention period.

Based on the above, when a pharmaceutical/medical device/other types of healthcare products are marketed, the relevant entity should firstly comply with the requirements of the general personal information protection regulations when it comes to post-marketing data, especially pharmacovigilance data. At the same time, in the event of a conflict between personal information protection and pharmacovigilance-related laws, the pharmacovigilance-related laws should take precedence.

**11. In your jurisdiction, is health related personal information regulated more strictly, or regulated differently than other personal information? If so, how is personal health data defined in your jurisdiction, and how is it regulated?**

Health-related personal information is classified as sensitive personal information under the PIPL and should be protected in accordance with the relevant provisions of the PIPL. Under the PIPL, the processing of sensitive personal information is subject to the following more stringent requirements:

- data handlers shall only process sensitive personal information if there is a specific purpose and a sufficient necessity, and when stringent protective measures are in place;
- specific consent shall be obtained from individuals when processing sensitive personal information unless otherwise specified by other laws and regulations.
- Article 30 of the PIPL provides that before processing sensitive personal information, the data handler shall notify the individuals of the necessity for processing their sensitive personal information; and
- Before processing sensitive personal information, the data handler shall carry out the protection impact assessment.

**12. In your jurisdiction, is medical data/healthcare data (e.g. data generated by medical institutions and healthcare administrative departments in the process of disease prevention and treatment, such as medical records, population health information etc.) more strictly regulated or regulated differently than other types of data? If so, how is medical data/healthcare data defined in your jurisdiction, and how is it regulated?**

Under Chinese law, there currently is no uniform definition of medical data/healthcare data, and regulations on its management are scattered across different laws. Nevertheless, this type of data is generally referred to as data generated by medical institutions and healthcare administrative departments in the process of disease prevention and treatment. Such data may include personal information, such as the health-related personal information in question 11, personal medical records, or data that does not involve personal information, such as public health data or healthcare

big data. The common feature of such data is that it is generally managed by healthcare institutions or healthcare administrative departments.

The management of this type of data in China is currently scattered in the *Measures for the Management of Population Health Information (for trial implementation)* (the "**Population Health Information Measures**"), implemented in 2014; the *Management Standards for the Application of Electronic Medical Records (for trial implementation)* (the "**Electronic Medical Records Measures**"), implemented in 2017; and the *Measures for the Management of National Health Care Big Data Standards, Security and Services (for trial implementation)* (the "**Health Care Big Data Measures**"), implemented in 2018.

Firstly, the Population Health Information Measures regulates health information such as basic population information, health service information and other population health information generated by medical and healthcare service providers. Among others, the main requirements are:

— Graded storage and disaster-tolerant backup requirements: the data holders are required to store population health information in a graded and classified manner according to the importance and sensitivity of the data, and in accordance with the national unified plan.

— No cross-border transfer: population health information shall not be stored or hosted in servers outside of China.

— Responsibility for entrusted storage: where other institutions are entrusted to store or operate and maintain population health information, the entrusted institution shall assume responsibility for the management and security of the population health information.

Secondly, the Electronic Medical Records Measures contains further requirements regarding electronic medical record data, which occupies a central position in medical data. These requirements cover the establishment, recording, modification, use, preservation, and management of electronic medical records. The main requirements include, but are not limited to:

— Length of medical record retention: Outpatient electronic medical records should be kept for not less than 15 years; inpatient electronic medical records should be kept for not less than 30 years. As with the pharmacovigilance record keeping requirement in question 10, this requirement may conflict with the patient's right to request the deletion of personal information under the PIPL. In this case, the requirements of the electronic medical records data storage should prevail.

— Copy of records: Medical institutions should provide applicants with the service of copying electronic medical records. This provision is consistent with the right of data subjects to access and copy their personal information under the PIPL. However, the Electronic Medical Records Measures set out more specific requirements for such rights, such as that the copied electronic medical record document should be independently readable and that the printed paper version of the electronic medical record should be stamped with the medical institution's special seal for medical record management.

In addition to the above two regulations, China also implemented the Health Care Big Data Measures in 2018. Unlike the other laws, which were implemented in 2014 and 2017 respectively, the Health Care Big Data Measures were enacted after the

implementation of the PRC Cybersecurity Law. The main features include the following:

— Broader scope: the Health Care Big Data Measures defines "big data on healthcare" as "data related to healthcare generated in the process of disease prevention and treatment and health management of people". Therefore, this kind of data includes not only individual healthcare data directly generated in the process of disease diagnosis, prevention, treatment, and health management, but also macroscopic data obtained from the statistics, processing, and analysis of a large number of individuals' disordered and scattered healthcare data.

— Secondly, it sets out more detailed requirements than the Population Health Information Measures, for the management of data.

  • In terms of the storage security of healthcare big data, the requirements of the Health Care Big Data Measures mainly include the adoption of security measures, such as data classification, important data backup, encryption and authentication, and the establishment of a reliable data disaster recovery and backup mechanism.

  • It is important to note that the Health Care Big Data Measures clearly require that healthcare big data should be stored on servers within the country, and if there is a need to transmit it outside the country, it should be subject to security assessment and audit in accordance with relevant laws, regulations, and requirements.

  • As far as data development and cooperation are concerned, the commissioning and entrusted data processing parties shall be jointly and severally liable for the management and security responsibilities of healthcare big data.

**13. Is data related to human genetic resources more strictly regulated or regulated differently than general personal information? If so, how is data related to human genetic resources defined in your jurisdiction, and how is it regulated?**

Human genetic resources information ("**HGR Information**") refers to information generated from the use of human genetic materials (e.g. organs, tissues and cells containing human genes). According to the latest interpretation of the competent human genetic resources management authority, information which is generated from human genetic materials, but does not contain human genes data or genomic data, is not considered as "HGR Information".

Currently, HGR Information is mainly governed by the *Biosafety Law* and the *Human Genetic Resources Management Regulations*. The most important of these requirements include:

— **Specific consent**: Specific consent should be obtained before HGR Information is collected, stored, and utilised.

— **Filing requirements**: Before HGR Information can be made available or open for use to any foreign parties, a filing should be made to the Ministry of Science and Technology and a backup copy of the information shall be submitted; and

— **Security review requirements**: In carrying out the second point above, if it may affect the public health, national security and social public interest of China, the filing requirements must also pass the security review organized by the Ministry of Science and Technology.

**14. In addition to the above, in your jurisdiction, is there any life sciences & healthcare related data that is regulated differently than data in other sectors? If so, what is this data, and how is it regulated?**

The above answers have largely covered the main features of life sciences & healthcare related data management, so we have nothing specific to add. However, we would like to make the following general comment - there is currently no complete, logical, and clear system for the management of life sciences & healthcare related data in China. A large number of the regulations cited in this questionnaire were issued prior to the introduction of the 2017 Cybersecurity Law and the PIPL, and by the regulators of the life sciences & healthcare sector, rather than the data management authorities. Therefore, there are duplications and contradictions between these regulations and the Cybersecurity Law, the PIPL, and even within each regulation. We would like to remind all parties to carefully identify and apply the relevant regulations in the context of their own business practices. In addition, we look forward to the introduction of more systematic regulations for the life sciences & healthcare industry in China in the future.

# India

## General questions

1. **Applicable legislation governing data protection in your jurisdiction, for both personal data and non-personal data?**

   Currently, India does not have a comprehensive and dedicated data protection legislation. Some provisions of the Information Technology Act 2000, as amended from time to time ("**IT Act**") and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 ("**SPDI Rules**") framed under it deal with protection of personal information ("**PI**") and sensitive personal data and information ("**SPDI**") on a sector neutral basis.

   Apart from the IT Act and SPDI Rules, regulations, directives and licence conditions issued by certain sectoral regulators in relation to payment systems, telecom, insurers, etc. stipulate certain data protection obligations.

   In India, there has been considerable traction with regard to data protection in recent times. In 2019, the Government of India presented the Personal Data Protection Bill, 2019 ("**PDP Bill**") in the Parliament which was later referred to a Joint Parliamentary Committee ("**JPC**") for a detailed review. On December 16 2021, the JPC tabled its report in Parliament with various recommendations and modifications to the PDP Bill, which, inter alia, includes expansion of the scope to cover both personal and non-personal data pursuant to which the PDP Bill has been rechristened as 'Data Protection Bill, 2021' ("**DP Bill**"). The DP Bill is currently awaiting deliberations in the Parliament.

2. **Who is/ are the regulator(s) in your jurisdiction for data protection?**

   At present, there is no dedicated regulator / authority responsible for data protection in India.

   The DP Bill envisages the constitution of a Data Protection Authority of India ("**DPAI**") for enforcement of its provisions.

3. **Who are governed by the data protection legislation in your jurisdiction?**

   The SPDI Rules do not recognise the concepts of data controllers and data processors, and do not use these or equivalent terms. Instead, the SPDI Rules govern all body corporates that collect and process PI and SPDI from information

providers. Body corporates have been defined as companies (including firms, sole proprietorships or other association of individuals) engaged in commercial or professional activities.

In contrast, the DP Bill clearly recognises such concepts and assigns data protection roles to parties. As per the DP Bill, any person that determines the purpose and means of processing of personal data (including sensitive personal data or any other subsets of personal data) would be classified as a 'data fiduciary' and person who processes such data on behalf of a data fiduciary would be classified as a 'data processor'.

**4. Is there an extraterritorial application effect under the data protection legislation in your jurisdiction?**

The IT Act has extra-territorial operation and applies "to any offence or contravention committed outside India by any person irrespective of his nationality", as long as the act constituting the offence or contravention involves a "computer" or "computer system" or "computer network" located in India. Moreover, the SPDI Rules cast obligations on a "body corporate" that processes SPDI, and the definition of "body corporate" under the IT Act does not restrict this to entities incorporated within India only.

The provisions of the DP Bill will be applicable to the processing of personal data (including sensitive personal data) by data fiduciaries and data processors not present in India if such processing is in connection with: (i) any business carried out in India; (ii) any systematic activity of offering goods and services to information providers within India; (iii) any activity which involves the profiling of information providers within India; and (iv) the processing of non-personal data including anonymised personal data.

**5. What are the key aspects to look to when processing personal data in your jurisdiction?**

In respect of PI (not being SPDI), Section 72-A of the IT Act becomes applicable. Under Section 72-A of the IT Act, PI (obtained as part of providing services under a lawful contract) may be disclosed to a third party, only on the basis of: (i) consent of the information provider; or (ii) if the disclosure is as per the terms of a contract.

Collection and subsequent handling of SPDI will be subject to compliances under the SPDI Rules as briefly described under Question 3 (Questions specific to life sciences & healthcare sector).

**6. What are the key aspects to look to when processing non-personal data in your jurisdiction?**

Applicability of the IT Act and SPDI Rules is limited to processing of PI and SPDI. Processing of non-personal data is not specifically governed by any law in India at present.

Although the scope of the DP Bill includes certain aspects of regulation of non-personal data along with personal data, conditions and measures to be implemented while collecting and processing non-personal data will be as per regulations to be framed once the DP Bill becomes enacted law.

**7. Is there requirement for data localisation requirement in your jurisdiction?**

The IT Act and SPDI Rules do not specifically require PI and / or SPDI to be stored within India.

However, certain sectoral laws and regulations require data localization. As examples:

- The Reserve Bank of India's Directive 2017-18/153 (April 6, 2018) issued under the Payment and Settlement Systems Act 2007 ("**Directive**"): Paragraph 2(i) of the Directive requires covered organizations to store payment data within India.
- The IRDAI (Maintenance of Insurance Records) Regulation 2015 ("**Regulation**"): Paragraph 3(9) of the Regulation requires covered organizations to store data relating to all policies issued and all claims made in India in data centres located in India.

**8. What are the requirements for cross-border transfer of data in your jurisdiction?**

According to the SPDI Rules, SPDI may be transferred by the collecting entity to an entity in another jurisdiction, provided that the transferee entity ensures the same level of data protection that is adhered to by the transferor under the SPDI Rules. Further, the transfer is allowed only if it is necessary for the performance of a lawful contract or where the provider of SPDI has consented to such data transfer. There are no requirements for cross border transfer of data for personal information under the IT Act except as provided in response to Question 5 above.

# Questions specific to the life sciences & healthcare sector

**9. From the perspective of personal data protection, during the clinical trial of a pharmaceutical/medical device/other types of healthcare products, how is the clinical trial data regulated? Does the general requirements in the questions above apply, or is clinical trial data regulated differently? If not, how is it differently regulated?**

Collection of data from clinical trial subjects ("**Subject(s)**") will be subject to provisions set out under the Third Schedule of the New Drugs and Clinical Trials Rules 2019 ("**Clinical Rules**"). As per the Clinical Rules, in all clinical trials, a freely given, informed, written consent is required to be obtained from each Subject, after informing them verbally about the clinical study, as well as by using a patient information sheet, in a language that is non-technical and understandable by the Subject. The Subject's consent must be obtained in writing using an 'informed consent form'. The Clinical Rules also provide the essential elements that are to be included in the Subject's informed consent form, including a format for the informed consent form. Such essential elements include description of any reasonably foreseeable risks or discomforts to the Subject; disclosure of specific appropriate alternative procedures or therapies available to the Subject; statement describing the extent to which confidentiality of records identifying the Subject will be maintained and who will have access to Subject's medical records; consequences of a Subject's decision to withdraw from the research and procedures for orderly termination of participation by Subject, etc.

In addition to the same, the investigator (i.e., the person responsible for conducting clinical trials at the clinical trial site) of the clinical trial or bioequivalence/bioavailability study is required to inter alia give an undertaking that he/she/they will maintain confidentiality of the identification of all participating subjects and assure security and confidentiality of study data in the said clinical trial or bioequivalence/bioavailability study.

In cases where a Subject is unable to give informed consent, the same may be obtained from a legally acceptable representative. Further, in case of clinical trials on paediatrics, where the Subjects are dependent on their parent or legal guardian to assume responsibility for their participation in clinical studies, written informed consent will need to be obtained from such parent or legal guardian.

**10. From the perspective of personal data protection, after the pharmaceutical/medical device/other types of healthcare products is marketed, how is the post-marketing data (for example, pharmacovigilance data) regulated? Does the general requirements in the questions above apply? If not, how is it differently regulated?**

The Clinical Rules do not prescribe any additional measures for regulation of post-marketing data specifically. Please, however, note that the entire pharmacovigilance system in the post-marketing surveillance stage is required to be managed by qualified and trained personnel, and the officer in-charge of collection and processing of data under the pharmacovigilance system is mandatorily required to be a medical officer, or a pharmacist trained in collection and analysis of such data.

**11. In your jurisdiction, is health related personal data related more strictly regulated or regulated differently than other personal data? If so, how personal health data defined in your jurisdiction, and how is it regulated?**

Under the SPDI Rules, SPDI has been defined to mean personal data consisting of:

(i) password;

(ii) financial information such as bank account or credit card or debit card or other payment instrument details;

(iii) ***physical, physiological and mental health condition***;

(iv) sexual orientation;

(v) ***medical records and history***;

(vi) biometric information;

(vii) any detail relating to the above clauses as provided to the entity for providing service;

(viii) any information received by the entity under the above clauses for processing, stored or processed under lawful contract or otherwise;

provided that any information that is freely available or accessible in public domain or furnished under the Right to Information Act 2005 or any other law for the time being in force, shall not be regarded as SPDI for the purposes of the SPDI Rules.

Since health related data may include data in relation to physical, physiological and mental health condition, medical records and history of an information provider, collection, processing and transfer of such SPDI is subject to compliance with certain requirements as set out under the SPDI Rules. We have briefly described such compliances below:

— **Reasonable security practices and procedures**: Section 43-A of the IT Act mandates following of "reasonable security practices and procedures" in relation to SPDI. It shall be considered that the entity has implemented such reasonable security practices and procedures, if it implements security practices and standards and has comprehensive and documented information security programmes and policies that contain managerial, technical, operational and physical security control measures, which are proportionate to the information assets that the entity is seeking to protect. The International Standard IS/ISO/IEC 27001 relating to 'Information Technology-Security Techniques-Information

Security Management System–Requirements' is one of the standards specified under the SPDI Rules that may be implemented by the entity while handling SPDI.

- **Privacy policy**: Under the SPDI Rules, an entity that collects, receives, possesses, stores, deals or handles SPDI of an information provider, is required to publish a privacy policy on its website that addresses its handling of SPDI. Such privacy policy must contain clear and easily accessible statements of the entity's practices and policies.
- **Consent and Collection**: For collection of SPDI, an entity is required to obtain consent in writing from the provider of the SPDI. An entity is not permitted to collect SPDI unless the information is collected for a lawful purpose connected with a function or activity of the entity; and the collection of SPDI is considered necessary for that purpose.
- **Purpose limitation and retention**: Under the SPDI Rules, an entity is not permitted to use SPDI for any reasons other than those for which it has been collected and is not allowed to retain SPDI for a period longer than is required for the purposes for which the SPDI may lawfully be used or is otherwise required under any other law for the time being in force.
- **Disclosure of SPDI**: The SPDI Rules specify that apart from disclosure of SPDI sought by governmental agencies or where it is required for compliance with a legal obligation, the entity is required to obtain consent from the information provider, prior to disclosure of such information to a third party, unless such disclosure has been agreed to in an agreement between the parties.
- **Grievance Officer**: Under the SPDI Rules, the entity is required to designate a grievance officer for redressal of grievances in relation to SPDI and publish the name and contact details of such officer on its website.

**12. In your jurisdiction, is medical data/healthcare data (e.g. data generated by medical institutions and health care administrative departments in the process of disease prevention and treatment, such as medical records, population health information etc.) more strictly regulated or regulated differently than other types of data? If so, how is medical data/healthcare data defined in your jurisdiction, and how is it regulated?**

Medical data/healthcare data would be categorised as SPDI under the SPDI Rules. Please see our response to Question 4 above for further details.

**13. Is data related to human genetic resources more strictly regulated or regulated differently than general personal data? If so, how is data related to human genetic resources defined in your jurisdiction, and how is it regulated?**

Genetic data would be categorised as SPDI under the SPDI Rules. Please see our response to Question 4 above for further details.

**14. In addition to the above, in your jurisdiction, is there any life sciences & healthcare related data that are regulated differently than data in other sectors? If so, what are these data, and how are they regulated?**

Apart from the broad categories of SPDI mentioned above, there are no other specific categories of life sciences & healthcare related data that are regulated differently under Indian law.

# Korea

## General questions

1. **Applicable legislation governing data protection in your jurisdiction, for both personal data and non-personal data?**

   For personal data, the “Personal Information Protection Act (**PIPA**)” acts as a general law for collecting and utilizing personal data. For non-personal data, South Korea does not have a general law which covers non-personal data protection, however, certain data may be protected by Copyright Act and Unfair Competition Prevention and Trade Secret Protection Act, subject to meeting the necessary conditions under the law. Below we have focused on personal data related regulations.

2. **Who is/ are the regulator(s) in your jurisdiction for data protection?**

   The Personal Information Protection Commission (“**PIPC**”) is a central administrative body with the primary role of the protection and supervision of personal information and the legal ground for its establishment is stipulated in the PIPA.

3. **Who are governed by the data protection legislation in your jurisdiction?**

   The PIPA applies to any person (which can be an individual, a public agency, a corporate body, or an organization), that either directly or indirectly (through a third party) processes the data subject's personal data file for its business purposes. “Processing” is defined under the PIPA as the “collection, creation, storage, retention, processing, editing, search, outputting, rectification, restoration, use, provision, disclosure, or destruction of personal data or any other action similar to any of the preceding.”

4. **Is there an extraterritorial application effect under the data protection legislation in your jurisdiction?**

   The PIPA does not explicitly define its territorial or extraterritorial scope. However, the interpretation of the regulatory authority is that if a foreign entity collects personal data in Korea, it would be subject to the PIPA, even if other steps of the processing or storing takes place outside of Korea.

## 5. What are the key aspects to look to when processing personal data in your jurisdiction?

- The privacy regime of South Korea is heavily reliant on the consent of the data subject. Under the PIPA, personal data controllers are required to obtain an explicit consent from the data subject before collecting, using, and providing third parties' personal information, subject to certain exceptions. Also, certain types of information, including “sensitive information” (which includes health information), a separate consent should be obtained.
- The PIPA stipulates various security requirements, data breach requirements and obligations such as appointing a Chief Privacy Officer (“CPO”) and disclosing the Privacy Policy.
- Personal information should, in most situations, be processed pursuant to the original purpose explained to the data subject at the time of data collection and with the consent of the data subject. In certain limited circumstances, personal information may be processed for purposes other than the initial purpose that was explained to the data subject, as stipulated by applicable laws and regulations.

## 6. What are the key aspects to look to when processing non-personal data in your jurisdiction?

As explained above, there is no “general” law governing the processing of non-personal data in general. However, under the Copyright Act of Korea, the creator of a database (which is defined as compilation of materials that are systematically arranged or composed, so that they may be individually accessed or retrieved) is granted protection by a right similar to copyright (right of copy, distribution, broadcasting or transmission of the database). In some cases, data can be protected by Unfair Competition Prevention and Trade Secret Protection Act. This Act defines certain unfair usage of data as “act of unfair competition” and forbids such act, some of the usage stipulated in the Act are:

1) An act of acquiring data by theft, deception, fraudulent access, or other illegal means by an unauthorized person, or using or disclosing such acquired data;
2) An act of using, disclosing, or providing data to a third party for the purpose of obtaining illegal profits or causing damage to the data holder by a person who has access to the data due to a contractual relationship or other legal basis;
3) acquiring data or using the data while being aware that the data has been acquired through 1) or 2) above.

## 7. Is there requirement for data localisation requirement in your jurisdiction?

There are no general law for data localization of the personal data. However, certain sectors, such as financial sector has industry-specific data localization requirements.

## 8. What are the requirements for cross-border transfer of data in your jurisdiction?

In general, cross-border transfer of personal information requires explicit consent from the data subject to provide personal data to a third party located overseas. However, in the case of “entrustment” of data processing to the third party (i.e. transfer of date in the context of a controller – processor relationship), an explicit consent is not required to the extent the relevant information is disclosed in the privacy policy of the data controller.

# Questions specific to the life sciences & healthcare sector

**9. From the perspective of personal data protection, during the clinical trial of a pharmaceutical/medical device/other types of healthcare products, how is the clinical trial data regulated? Does the general requirements in the questions above apply, or is clinical trial data regulated differently? If not, how is it differently regulated?**

— The general requirements in the questions above apply. In other words, the PIPA applies to the personal data collected during the process of clinical trial of a pharmaceutical/medical device, thus separate explicit consent should be obtained for the collection, transfer and processing of such personal data.

— There are relevant regulations regarding the clinical trial of pharmaceutical/medical device under the respective industry laws. Please see below.

(1) The Pharmaceutical Affairs Act regulates procedures regarding the clinical trial of pharmaceuticals, and it stipulates that the data should be processed pursuant to the PIPA:

| Article 34-2 (4) of the Pharmaceutical Affairs Act |
| --- |
| "The Minister of Food and Drug Safety and an institution conducting clinical trials may process information on health prescribed in Article 23 of the Personal Information Protection Act and data containing personally identifiable information prescribed in Article 24 of that Act, after obtaining consent from the data subjects, to perform the affairs regarding the selection, management, etc. of subjects of clinical trials. In such cases, the Minister of Food and Drug Safety and the institution conducting clinical trials shall protect the relevant information in accordance with the Personal Information Protection Act." |

(2) Medical Devices Act regulates procedures regarding the clinical trial of the medical device, however it does not stipulate any specifics regarding the data collected during the clinical trial. Thus, general requirements of the PIPA will apply to the personal data collected.

**10. From the perspective of personal data protection, after the pharmaceutical/medical device/other types of healthcare products is marketed, how is the post-marketing data (for example, pharmacovigilance data) regulated? Does the general requirements in the questions above apply? If not, how is it differently regulated?**

Under the PIPA, there are no special provisions regarding post-marketing data. Generally speaking, the data controller is able to process the data for as long as there is valid consent of the data subject. With that said, the PIPA also states that the personal information controller may collect and transfer personal information without the explicit consent of the data subject when such processing is inevitable for the fulfillment of legal obligations. The Pharmaceutical Affairs Act stipulates that the manufacturers, importers, importers, and drug wholesalers who have obtained permission for drugs, etc. shall report cases of disease, disability, death, or other cases of safety and validity of drugs prescribed by Prime Minister's Decree to the head of the Drug Safety Management. Therefore, there are certain cases where the

explicit consent obligations do not apply for post-marketing personal data, however the cases are quite limited to the ones stipulated in the law.

**11. In your jurisdiction, is health related personal data related more strictly regulated or regulated differently than other personal data? If so, how personal health data defined in your jurisdiction, and how is it regulated?**

— Yes. As briefly mentioned above, PIPA stipulates "sensitive information" as a special personal data which is more strictly regulated. Sensitive information includes data related to race or ethnics, political opinions, genetic data, biometric data, sex life or sexual orientation, health and medical records and etc. Most of the health related data is defined as "sensitive data" under the PIPA and more strictly regulated than other personal data.

— For example, to collect the sensitive data, the controller must obtain explicit separate consent with notification of the specific data collected, the purpose of collection and the retention period.

**12. In your jurisdiction, is medical data/healthcare data (e.g. data generated by medical institutions and health care administrative departments in the process of disease prevention and treatment, such as medical records, population health information etc.) more strictly regulated or regulated differently than other types of data? If so, how is medical data/healthcare data defined in your jurisdiction, and how is it regulated?**

Yes. The Medical Service Act regulates the medical institution's obligation to manage and protect the medical records of patients. According to the Medical Service Act, transfer or sending of the medical record outside the medical institution is strictly regulated. At the same time, the Act stipulates that except as expressly provided for in the Medical Service Act, matters necessary for the establishment and operation of a medical record transmission system shall be governed by the PIPA.

**13. Is data related to human genetic resources more strictly regulated or regulated differently than general personal data? If so, how is data related to human genetic resources defined in your jurisdiction, and how is it regulated?**

Yes. About genetic information, the Bioethics and Safety Act defines genetic information as information regarding the genetic characteristics of an individual, which is obtained by analyzing human body components or biospecimens (Article 2, Subparagraphs 11 and 14). The Bioethics and Safety Act specifically forbids the medical institution from providing genetic information to anyone other than the patient him/herself except for certain cases.

> Article 46 (3) of the Bioethics And Safety Act
>
> "No medical institution shall include genetic information in medical records, therapy records, etc. provided to any person other than the patient himself or herself pursuant to Article 21 (3) of the Medical Service Act; provided, that the foregoing shall not apply where another medical institution requests such records for the purpose of diagnosis or treatment of the same disease as the disease of the patient involved and measures for protecting personal information are taken."

**14. In addition to the above, in your jurisdiction, is there any life sciences & healthcare related data that are regulated differently than data in other sectors? If so, what are these data, and how are they regulated?**

— As explained above, health related data are considered as "sensitive data" under the PIPA, which require specific consent from the data subjects after informing them of the sensitive nature of the information.

- The Bioethics and Safety Act provides that express consent of the data subject is required prior to conducting clinical studies, unless such information may be anonymized. According to the Guidelines for Use of Health & Medical Information published by the Ministry of Health and Welfare, the term “anonymized data” under the Bioethics and Safety Act is interpreted to include the concept of “pseudonymised information” under the PIPA.
- For your information, in light of the newly added provisions to PIPA in 2020, personal information controllers may process pseudonymised information without the consent of data subjects for the purposes of statistics, scientific research and archiving in the public interest. Such pseudonymised information may then also be provided to third parties without the consent of data subjects, as long as such provision is within the scope of the above purposes. However, in order to process pseudonymised information, various measures to ensure safety (managerial, technical and physical security measures) specified in the Presidential Decree must be in place, regarding which the PIPC published the Guidelines on Processing Pseudonymised Data to serve as general guidance.

# Singapore

## General questions

1. **Applicable legislation governing data protection in your jurisdiction, for both personal data and non-personal data?**

   For personal data, the Personal Data Protection Act 2012 ("**PDPA**") is the applicable legislation. Non-personal data is protected under the common law obligation of confidence or under a contract such as a non-disclosure agreement ("**NDA**").

2. **Who is/are the regulator(s) in your jurisdiction for data protection?**

   The Personal Data Protection Commission ("**PDPC**") is the regulator.

3. **Who are governed by the data protection legislation in your jurisdiction?**

   The PDPA governs the collection, use and disclosure of personal data by "organisations", which include any individual, company, association, or body of persons, corporate or unincorporated. Further, it does not matter whether the organisation is formed or recognised under Singapore law, or whether it is a resident, or has an office in Singapore. However, no data protection obligations are imposed on public agencies or individuals acting in a personal capacity or acting in the course of employment within an organisation.

4. **Is there an extraterritorial application effect under the data protection legislation in your jurisdiction?**

   Yes, the PDPA has extraterritorial effect and applies to all organisations that collect, use and/or disclose personal data from individuals in Singapore, regardless of whether the organisations have a physical presence or are registered in Singapore.

5. **What are the key aspects to look to when processing personal data in your jurisdiction?**

   Organisations that process personal data must comply with ten key obligations under the PDPA:

   - **Consent Obligation**: an organisation must obtain the consent of the individual before collecting, using or disclosing his personal data for a purpose.
   - **Purpose Limitation Obligation**: an organisation may 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.

- **Notification Obligation**: an organisation must notify the 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 of the personal data.
- **Access and Correction Obligation**: an organisation must, upon request, (i) provide an individual with his or her personal data in the possession or under the control of the organisation 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 an individual's personal data that is in the possession or under the control of the organisation.
- **Accuracy Obligation**: an organisation must make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete if the personal data is likely to be used by the organisation to make a decision that affects the individual concerned or disclosed by the organisation to another organisation.
- **Protection Obligation**: an organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent (i) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (ii) the loss of any storage medium or device on which personal data is stored.
- **Retention Limitation Obligation**: an organisation must cease to retain documents containing personal data, or remove the means by which the personal data can be associated with particular individuals as soon as it is reasonable to assume that (i) the purpose for which the personal data was collected is no longer being served by retention of the personal data; and (ii) retention is no longer necessary for legal or business purposes.
- **Transfer Limitation Obligation**: an organisation must not transfer personal data to a country or territory outside Singapore except in accordance with the requirements prescribed under the PDPA, to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under the PDPA.
- **Data Breach Notification Obligation**: an organisation must assess whether a data breach is notifiable and notify the affected individuals and/or the Commission where it is assessed to be notifiable.
- **Accountability Obligation**: an organisation must implement the necessary policies and procedures in order to meet its obligations under the PDPA and shall make information about its policies and procedures publicly available.

### 6. What are the key aspects to look to when processing non-personal data in your jurisdiction?

Processors of non-personal data should:

- ensure that such non-personal data cannot be used in combination with other information to identify an individual, as such non-personal data will in fact be "personal data" regulated under the PDPA.
- ensure that they do not make unauthorised use of information that has a quality of confidence and that was imparted under circumstances giving rise to an obligation of confidence.
- ensure that the non-personal data is not subject to an NDA.

**7. Is there a requirement for data localisation in your jurisdiction?**

No, there are no data localisation requirements under the PDPA.

**8. What are the requirements for cross-border transfers of data in your jurisdiction?**

Cross-border transfers of data must be done in accordance with prescribed requirements to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under the PDPA. Organisations should implement policies and procedures on when and how personal data may be transferred out of Singapore. This may include putting in place a suitable contract between the organisation and the foreign recipient of the personal data or, in the case of intra-corporate transfers, binding corporate rules. Further, consent is generally required from the data subjects.

# Questions specific to the life sciences & healthcare sector

**9. From the perspective of personal data protection, during the clinical trial of a pharmaceutical/medical device/other types of healthcare products, how is the clinical trial data regulated? Do the general requirements in the questions above apply, or is clinical trial data regulated differently? If not, how is it differently regulated?**

Insofar as clinical trial data contains personal data, the PDPA does not regulate such data differently and the general data protection obligations stated above apply. However, the PDPC has advised organisations to implement policies that ensure appropriate levels of security for personal data of varying levels of sensitivity. For example, in the case of *Aviva Ltd* [2018] SGPDPC 4, the PDPC regarded medical conditions to be sensitive personal data and, in assessing the breach and determining the directions to be imposed, held that the failure to protect such information was an aggravating factor.

**10. From the perspective of personal data protection, after the pharmaceutical/medical device/other types of healthcare products is marketed, how is the post-marketing data (for example, pharmacovigilance data) regulated? Do the general requirements in the questions above apply? If not, how is it differently regulated?**

To the extent that post-marketing data of healthcare products contain personal data, such data is not regulated differently and the general data protection obligations stated above apply.

**11. In your jurisdiction, is health related personal data related more strictly regulated or regulated differently than other personal data? If so, how is personal health data defined in your jurisdiction, and how is it regulated?**

No, health-related data is not regulated differently under PDPA. However, the data protection obligations relating to health-related data may be affected by other healthcare-related legislation. For example, under the Retention Limitation Obligation, personal data must be removed as soon as it is reasonable to assume that retention is no longer necessary for legal purposes. However, the Private Hospitals and Medical Clinics Regulations require the keeping and maintaining of proper medical records. This would constitute the “legal purpose” under the PDPA that mandates further retention of data.

**12. In your jurisdiction, is medical data/healthcare data (e.g. data generated by medical institutions and health care administrative departments in the process of disease prevention and treatment, such as medical records, population health information etc.) more strictly regulated or regulated differently than other types of data? If so, how is medical data/healthcare data defined in your jurisdiction, and how is it regulated?**

No, personal data that is medical/healthcare data is not generally regulated differently under PDPA. However, as highlighted in the PDPC's advisory guidelines for the healthcare sector, the Consent Obligation in the context of medical data/healthcare data should take into account specific healthcare related considerations:

- The voluntary provision of personal data through the presentation of oneself for medical examination may constitute deemed consent to the collection, use and disclosure of personal data for the purpose of the visit as well as any associated examinations and subsequent follow-up consultations.
- Under the Infectious Diseases Act, medical practitioners are required to notify the Director of Medical Services within a prescribed time and form if the practitioner has reason to believe or suspect that any person attended or treated by him is suffering from an infectious disease or is a carrier of such disease. In such a case, the medical practitioner is not required under the PDPA to obtain the consent of the individual to notify the Director in compliance with the Infectious Diseases Act.

**13. Is data related to human genetic resources more strictly regulated or regulated differently from general personal data? If so, how is data related to human genetic resources defined in your jurisdiction, and how is it regulated?**

No, personal data related to human genetic resources is not regulated differently under the PDPA.

**14. In addition to the above, in your jurisdiction, is there any life sciences & healthcare related data that are regulated differently than data in other sectors? If so, what are these data, and how are they regulated?**

No, there are no other life sciences & healthcare related personal data that are regulated differently from personal data in other sectors.

# Taiwan

## General questions

**1. Applicable legislation governing data protection in your jurisdiction, for both personal data and non-personal data?**

*The Personal Data Protection Act (PDPA)* is the primary law regulating personal data protection. In addition to the *PDPA*, the Legislative Yuan has also enacted certain special data protection requirements in some sector-specific laws, such as *Medical Care Act, Regulations on Human Trials*, *Regulations for Good Clinical Practice*, *Regulations for the Management of Drug Safety Surveillance*, and *Human Biobank Management Act*, etc.

On the other hand, it is the *Cyber Security Management Act (CSMA)* is a primary and general law regarding information, i.e. personal data and non-personal data. *CSMA* is applicable in the service to be used to collect, control, transmit, store, circulate, delete information or to make other processing, use and sharing of such information by governmental agencies and specific private sectors, i.e. critical infrastructure providers, government-owned enterprises and government-endowed foundations. In practice, *CSMA* applies only to governmental agencies and specific private sectors such as a government medical center, which is principally irrelevant to general private entities. Therefore, except for Item 6 below, we will mainly focus only on personal data protection under the *PDPA* or other laws and regulation in the rest of section.

**2. Who is/ are the regulator(s) in your jurisdiction for data protection?**

The regulators in our jurisdiction for personal data protection are the central government authority in charge of the industry concerned (for example Retail Sales of Drugs, Medicines and Cosmetics are regulated by Ministry of Health and Welfare) or the local government. Both central and local governmental authorities have the power to:

(1) carry out audits and inspections on non-governmental agencies;

(2) request information;

(3) demand rectification; and

(4) impose administrative penalties against non-governmental agencies for non-compliance with the *PDPA*.

According to *CSMA*, the regulator in our jurisdiction for information is the Executive Yuan.

### 3. Who are governed by the data protection legislation in your jurisdiction?

For the personal data protection, the *PDPA* regulates any person, i.e. governmental agencies and all private sector entities, who collects, processes or uses personal data.

As for information including non-personal data, *CSMA* regulates governmental agencies and specific private sectors, i.e. critical infrastructure providers, government-owned enterprises and government-endowed foundations.

### 4. Is there an extraterritorial application effect under the data protection legislation in your jurisdiction?

According to the principle of territoriality, any person who violates *PDPA* in our country, whether a national or a foreigner, should be subject to PDPA. In addition, any person who collects, processes or uses personal data of our nationals in another country also is subject to *PDPA* based on personality of laws.

### 5. What are the key aspects to look to when processing personal data in your jurisdiction?

The key aspects of the *PDPA* mainly include: (1) the general requirements for the collection and processing of personal data by private entities and governmental agencies, (2) the requirements to be informed when obtaining the consent of the personal data subject (i.e. the person whose personal data is collected and processed), (3) the security matters to be handled by those who keep personal data, and (4) damages and penalties are the key aspects of the *PDPA*, which are further introduced as follows:

According to the *PDPA*, the collecting, processing of personal data (except sensitive personal data) by private entities shall be with and shall be within the specified purpose, and shall meet one of the following statutory matters:

(1) it is based on laws that specifically provides that the data collector can collect personal data without consent;

(2) it is based on contractual or quasi-contractual relationships between the data collector and the data subject;

(3) the data subject voluntarily publishes his/her personal data;

(4) it is necessary for statistical or academic research by an academic research institute for the purpose of public interest, and the personal data is processed or disclosed in a manner that does not permit the identification of the data subject;

(5) the data subject's consent is obtained;

(6) it is necessary for the public interest;

(7) the personal data is obtained from a generally accessible source, unless the interest of the data subject takes priority over that of the data collector or data controller; or

(8) the personal data collection and processing do not harm the rights and interests of the data subject.

As for governmental agencies, the collecting, processing of personal data (except sensitive personal data) shall be with and shall be within the specified purpose, and shall meet any of the following statutory matters:

(1) where it is expressly required by law;

(2) where it is necessary for ensuring national security or furthering public interest;

(3) where it is to prevent harm on life, body, freedom, or property of the data subject;

(4) where it is to prevent material harm on the rights and interests of others;

(5) where it is necessary for statistics gathering or academic research by a government agency or an academic institution for public interests; provided that such data, as processed by the data provider or as disclosed by the data collector, may not lead to the identification of a specific data subject;

(6) where it is for the data subject's rights and interests; or

(7) where consent has been given by the data subject.

For the consent of the data subject, it is given by a data subject after he/she has been informed by the data collector of the information required under the *PDPA*, i.e. (i) the name of the government or non-government agency; (ii) the purpose of the collection; (iii) the categories of the personal data to be collected; (iv) the time period, territory, recipients, and methods of which the personal data is used; (v) the data subject's rights under Article 3 and the methods for exercising such rights; and (vi) the data subject's rights and interests that will be affected if he/she elects not to provide his/her personal data.

Under the *PDPA*, any person in possession of personal data files shall take appropriate data protection measures, which may include conducting privacy, fairness or legitimate impact analyses and other measures, such as preventing personal data from being stolen, altered, damaged, destroyed or disclosed. Furthermore, the relevant business governmental authority may designate a private entity to set up a plan of security measures for the personal data or the disposal measures for the personal data upon the termination of business.

Last but not least, in case of violation of the *PDPA*, the personal data subject may claim for damages and restoration of reputation, and, for certain events, the violator shall be criminally liable for the corresponding illegal acts.

## 6. What are the key aspects to look to when processing non-personal data in your jurisdiction?

As we mentioned above, *CSMA* is a primary and general law regulating governmental agencies and specific private sectors. The *CSMA* is aimed at people's lives, economic activities, and public or national security that have a significant impact. The governmental agencies and specific private sectors are required to set up corresponding information security maintenance plans, establish notification and response mechanisms according to *Regulations on Classification of Cyber Security Responsibility Levels*, and accept relevant audits. For example, a government medical center is ranked as Level-A in its cyber security responsibility; therefore, its cyber security health diagnosis should conduct once a year and it shall deploy four persons on a full-time basis for dedicated cyber security personnel, etc.

## 7. Is there requirement for data localisation requirement in your jurisdiction?

There is no data localization requirement under Taiwan laws.

**8. What are the requirements for cross-border transfer of data in your jurisdiction?**

Cross-border transfer of personal data in Taiwan is based on the principle of "permitted in principle, prohibited by exception." Under the *PDPA*, the governmental authority in charge of the pertinent industry may limit international data transfers if:

(1) they involve important national interests;

(2) a national treaty or agreement specifies otherwise;

(3) the country receiving personal information lacks proper regulations towards the protection of personal information and it might harm the rights and interests of the data subject; or

(4) international transfers of personal information are made through an indirect method in which the provisions of the *PDPA* may not be applicable.

# Questions specific to the life sciences & healthcare sector

**9. From the perspective of personal data protection, during the clinical trial of a pharmaceutical/medical device/other types of healthcare products, how is the clinical trial data regulated? Does the general requirements in the questions above apply, or is clinical trial data regulated differently? If not, how is it differently regulated?**

The clinical trial data does not fall within the definition of personal data regarding healthcare under the *PDPA*. However, some other laws may apply.

"Healthcare" in *PDPA* shall mean medical histories and any other data pertaining to checkups or treatments implemented by physicians or other medical professionals for the purpose of treating, correcting or preventing diseases, harms or disabilities of human body or for other legitimate medical reasons, or shall mean other data produced from the prescription, medication, operation or disposition based on the findings of the above-mentioned checkups, which does not include clinical trial data.

First of all, the clinical trial data during the clinical trial of a pharmaceutical/medical device/other types of healthcare products is regulated under *Medical Care Act* and other relevant regulations. When performing human researches, medical institutions shall exercise due medical care and shall obtain the written consent of the subject of the test by clearly state the following: (i) Purpose and method of research; (ii) Possible risks and side effects; (iii) Expected results; (iv) Explanation of other possible treatment methods; (v) Subject's right to withdrawal of consent at any time; (vi) Research-related compensation for damages or insurance coverage; (vii) Confidentiality of the subject's personal information; and (viii) The preservation and reutilization of the subject's biological samples, personal data or derivatives thereof.

In addition, according to *Regulations on Human Trials*, the trial subject's biological samples, personal data, or derivatives shall be destroyed immediately upon completion of the human trial. The reutilization of aforesaid material(s) as subject to the trial subject's consent shall be reviewed and approved by the review board. A new written consent shall be obtained from the trial subject with regard to any non-delinked material(s).

Furthermore, if the trial is relevant to pharmaceutical clinical trial, *Regulations for Good Clinical Practice* further stipulates that records identifying the subject will be kept confidential and, to the extent permitted by the applicable laws and/or

regulations, will not be made publicly available. If the results of the trial are published, the subject's identity will remain confidential.

Given such, we believe that clinical trial data is regulated in a similar frame as *PDPA*, such as obtaining consent of the subject by clearly statement, however, there are still some differences in the requirements of specific laws and regulations.

**10. From the perspective of personal data protection, after the pharmaceutical/medical device/other types of healthcare products is marketed, how is the post-marketing data (for example, pharmacovigilance data) regulated? Does the general requirements in the questions above apply? If not, how is it differently regulated?**

If the post-marketing data do not involve personal data, i.e. de-identified data, it is irrelevant to personal data and is not subject to *PDPA*. However, according to *Regulations for the Management of Drug Safety Surveillance*, when the pharmaceutical dealers need to collect, process, or utilize personal data in order to conduct drug safety surveillance, they shall follow the requirements of the *PDPA* and its relevant regulations. For medical device, there are also the same regulations.

**11. In your jurisdiction, is health related personal data related more strictly regulated or regulated differently than other personal data? If so, how personal health data defined in your jurisdiction, and how is it regulated?**

Health related personal data is more strictly regulated and regulated differently than other personal data. Under the *PDPA*, "sensitive data" is defined as personal data regarding medical records, healthcare (i.e. medical treatment), genetic information, sexual life, health examinations and criminal record. Such sensitive data shall not be collected, processed or used unless the statutory requirements are satisfied, such as compliance with the laws and regulations, and obtaining written consent from the data subject.

As noted above, medical records and health examination records, i.e. health related personal data, fall within the definition of sensitive data under the *PDPA*, and the *PDPA* will apply. The regulation of sensitive data is more stringent, and in principle, the use of such data is prohibited, but only in the following cases:

(1) where it is expressly required by law;

(2) where it is within the necessary scope for a government agency to perform its statutory duties or for a non-government agency to fulfill its statutory obligation, provided that proper security and maintenance measures are adopted prior or subsequent to such collection, processing or use of personal data;

(3) where the personal data has been disclosed to the public by the data subject or has been made public lawfully;

(4) where it is necessary for statistics gathering or academic research by a government agency or an academic institution for the purpose of healthcare, public health, or crime prevention, provided that such data, as processed by the data provider or as disclosed by the data collector, may not lead to the identification of a specific data subject;

(5) where it is necessary to assist a government agency in performing its statutory duties or a non-government agency in fulfilling its statutory obligations, provided that proper security and maintenance measures are adopted prior or subsequent to such collection, processing, or use of personal data; or

(6) where the data subject has consented to the collection, processing and use of his/her personal data in writing, except where the collection, processing or use exceeds the necessary scope of the specific purpose, or where the collection,

processing or use based solely on the consent of the data subject is otherwise prohibited by law, or where such consent is not given by the data subject out of his/her free will.

**12. In your jurisdiction, is medical data/healthcare data (e.g. data generated by medical institutions and health care administrative departments in the process of disease prevention and treatment, such as medical records, population health information etc.) more strictly regulated or regulated differently than other types of data? If so, how is medical data/healthcare data defined in your jurisdiction, and how is it regulated?**

For medical data/healthcare data involving personal data, it is "sensitive data" regulated by *PDPA*, i.e., subject to more stringent controls. Please refer to Item 11 for further details.

However, one of exceptions is that if it is necessary for government agencies or academic institutions to collect statistical data or conduct academic research for health care, public health or crime prevention purposes, as long as such data is processed by the data provider or disclosure by the data collector would not identify a specific data subject.. Once court judgment ruled that National Health Insurance Administration of the Ministry of Health and Welfare provides personal health insurance information to the Ministry of Health and Welfare to establish the "Health and Welfare Data Science Center," which meets the requirements of such exception under the *PDPA*, since such information is not able to identify a specific subject by the way it is disclosed. Please note that this exception is now under the review by the Constitutional Court and further observation of the Constitutional Court's view on this point is important

Furthermore, according to the National Health Insurance Act, the insurer (ie, the Bureau of National Health Insurance of the Ministry of Health and Welfare) may require hospitals to provide certain personal data that is necessary for the insurer to carry out and administer the business of national health insurance. The obtaining of information by the insurer is also in accordance with the exception of the *PDPA*.

**13. Is data related to human genetic resources more strictly regulated or regulated differently than general personal data? If so, how is data related to human genetic resources defined in your jurisdiction, and how is it regulated?**

Data related to human genetic resources is more strictly regulated than general personal data and is protected under Article 6 of *PDPA* as "sensitive information," Such data should not be collected, processed or used, in principle, however, there are exceptions. Please refer to Item 11 for further details. In the event of collection with the written consent of the data subject, the person concerned shall be informed of the matters to be notified as stipulated in the *PDPA* and shall give his or her written consent to ensure that the "informed consent" is obtained. According to *Guidelines for Collection and Use of Human Specimens for Research*, except as provided for in the law, the collection of human specimens including genetic material for research use should be notified to the human specimen provider and their consent obtained. In principle, both the notification and consent should be in writing, supplemented by verbal notification so that the provider is aware of its contents.

**14. In addition to the above, in your jurisdiction, is there any life sciences & healthcare related data that are regulated differently than data in other sectors? If so, what are these data, and how are they regulated?**

In general, the main laws and regulations regarding life sciences & healthcare related data have been mentioned above. However, if there is any specific question, please

seek for advice from the local counsel as the application of laws and regulations may be determined on a case-by-case basis.

# Thailand

## General questions

1. **Applicable legislation governing data protection in your jurisdiction, for both personal data and non-personal data?**

   The main data protection legislation in Thailand is the Personal Data Protection Act B.E. 2562 (2019) ("PDPA") which was enacted and published in the Government Gazette on May 27, 2019. The law took full effect on June 1, 2022.

   There are also industry-specific personal data protection requirements for various sectors ("Specially Protected Sectors")—including healthcare and life sciences. There is a separate regime applicable to government entities, and there are also some laws/provisions which bind individuals engaging in certain professions/occupations, such as medical practitioners, pharmacists, druggists, midwives, nursing attendants, priests, advocates, lawyers, or auditors, and assistants or trainees in such professions, as well as government officials.

   People who suffer damage due to unauthorized disclosure of their personal data may claim against the responsible party in tort (under the Civil and Commercial Code); criminal charges (under the Penal Code) may also be possible, depending on the circumstances (e.g. criminal defamation, etc.).

   In relation to data which cannot be used to identify an individual, whether directly or indirectly (e.g., anonymized data), it would not be considered personal data and, thus, would not be subject to the provisions of the PDPA. However, non-personal data could still be subject to other applicable legislation, such as the law on trade secrets.

2. **Who is/ are the regulator(s) in your jurisdiction for data protection?**

   The Personal Data Protection Commission (PDPC) is the regulator under the PDPA.

   In the Specially-Protected Sectors, the regulators specific to those sectors may have some authority in respect of privacy matters in those sectors. For example, the Ministry of Public Health is empowered to issue regulations to govern the processing of health-related data. Other examples include the Securities and Exchange Commission, which is the regulator dealing with noncompliance with license conditions that concern privacy, and the Credit Information Protection Committee,

which has the authority to deal with noncompliance with privacy obligations under the Credit Information Business Act.

### 3. Who are governed by the data protection legislation in your jurisdiction?

Any person who acts as a data controller or data processor is subject to privacy obligations.

The PDPA defines “data controller” as a person or legal entity having authority to make determinations regarding the processing of personal data, and “data processor” as a person or legal entity that processes personal data on behalf of or pursuant to the instructions of the data controller.

The PDPA does provide exemptions from being subject to its provisions—for example, when the processing is for the personal interest or household activity of that person, or when the act is carried out by the government agencies responsible for maintaining state stability (including anti-money laundering and cybersecurity).

Within the Specially Protected Sectors, the parties subject to privacy obligations depend on the provisions of each law or regulation. For example, the National Health Act provides that all persons are subject to the obligations to keep personal health data confidential, and not disclose such data in a manner as to cause damage to an individual, unless otherwise provided therein. Another example is pursuant to regulations under the Securities and Exchange Act, licensees are obligated to address—as part of the application process—how they will protect personal data.

### 4. Is there an extraterritorial application effect under the data protection legislation in your jurisdiction?

Yes, the PDPA adopts the extraterritorial principle from the GDPR.

Data controllers and data processors located outside Thailand are subject to the PDPA if there is processing of the personal data of data subjects in Thailand, and it relates to the following activities:

- The offering of goods or services to data subjects in Thailand, irrespective of whether payment is made by the data subject; or
- The monitoring of the data subject’s behavior that takes place in Thailand.

### 5. What are the key aspects to look to when processing personal data in your jurisdiction?

In general, the PDPA only permits the processing of personal data where the lawful basis can be identified – for example, consent, legitimate interest, contractual obligations, legal obligations, etc.

The principles applicable to personal data processing under the PDPA include data minimization, purpose limitation, accuracy, storage limitation, lawfulness, fairness and transparency. These principles are not expressly indicated in the PDPA itself; however, these principles can be implied from the provisions of the PDPA.

The processing of certain categories of sensitive personal data (e.g., health data, biometric data, genetic data, or criminal records) is subject to more stringent requirements – for example, processing of the sensitive personal data will generally require explicit consent of the data subjects, unless another legal basis can be relied on.

Within the Specially Protected Sectors, some regulatory notifications set out further requirements in respect of the use and disclosure of personal data.

6. **What are the key aspects to look to when processing non-personal data in your jurisdiction?**

   As mentioned in Question 1 above, non-personal data could be subject to other legislation depending on the types of non-personal data and the purposes of processing of such non-personal data. It is also important to note that in the event the non-personal data is combined with other sets of data and, as a result, enables the identification of the data subject, whether directly or indirectly, such combined data will be regarded as personal data and thus, within the scope of the PDPA.

7. **Is there requirement for data localisation requirement in your jurisdiction?**

   There is no general data localization requirement in Thailand, except for certain specific businesses – for example, in relation to debit cards issued and used domestically.

8. **What are the requirements for cross-border transfer of data in your jurisdiction?**

   Generally, cross-border transfer is permitted if the destination country or the international organization that receives the personal data has adequate personal data protection standards in place, or if the cross-border transfer falls within any of the permitted activities prescribed by the PDPA—for example, when the data subject has been informed of the inadequacy of the personal protection standards of the destination country or the international organization and has granted consent to the cross-border transfer, or when an intra-group policy has been implemented for the cross-border transfer of personal data among group companies and/or affiliates, and such policy has been examined and certified by the Office of PDPC.

   As for the Specially Protected Sectors, such requirements may exist, depending on the sector. For example, the Credit Information Business Act contains restrictions on the transfer of information abroad. Also, regulations issued under the Telecommunications Business Act specify that a further regulatory notification may be issued to impose restrictions on the transfer of information abroad (thus far, such has not been issued).

# Questions specific to the life sciences & healthcare sector

9. **From the perspective of personal data protection, during the clinical trial of a pharmaceutical/medical device/other types of healthcare products, how is the clinical trial data regulated? Does the general requirements in the questions above apply, or is clinical trial data regulated differently? If not, how is it differently regulated?**

   The general requirements of the PDPA apply to personal data in clinical trials as well.

   There is no specific legislation governing human clinical trials in Thailand, though trial subjects are required to sign an informed consent form before commencement of clinical trials. The consent forms must emphasize that participation is voluntary and, therefore, subjects have the right to withdraw from the trial at any time.

10. **From the perspective of personal data protection, after the pharmaceutical/medical device/other types of healthcare products is marketed, how is the post-marketing data (for example, pharmacovigilance data)**

**regulated? Does the general requirements in the questions above apply? If not, how is it differently regulated?**

While the Food and Drug Administration (FDA) has issued notifications to impose obligations on the holders of licenses for the importation, distribution, or manufacture of drugs, medical devices, and healthcare products, such notifications merely stipulate the obligations of the license holders to report to the FDA on adverse events and the forms which must be used for such reports. However, the notifications do not prescribe any specific provisions or requirements on the processing of personal data and, therefore, the general requirements of the PDPA will still apply.

**11. In your jurisdiction, is health related personal data related more strictly regulated or regulated differently than other personal data? If so, how personal health data defined in your jurisdiction, and how is it regulated?**

According to Section 26 of the PDPA, health-related personal data is considered to be sensitive personal data and, therefore, the processing of health-related personal data will generally require explicit consent of the data subject, unless such processing can rely on another legal basis, such as vital interest, legal obligation under specific circumstances, etc. Under the PDPA, health-related personal data is treated the same as other categories of sensitive personal data.

The National Health Act does not define the term “health-related personal data”; however, it does define the term “health” as the state of a human being which is perfect in physical, mental, spiritual, and social aspects, all of which are holistic in balance, and therefore, health-related personal data could be implied to mean the data of a person which relates to such state of a human being.

Health records which are retained, managed, used, and disclosed by the Ministry of Public Health, government, and private organizations are regulated by the Regulation of the Ministry of Public Health Re: Protection and Management of Health-Related Data of Individuals (“MoPH Notification”), which defines the term “health-related personal data” as any information or thing in the form of documents, files, reports, writings, charts, maps, drawings, photographs, film, video recordings or audio recordings using electronic devices, or any other methods which make a record of health-related data, which enables the identification of an individual, and it shall also include other data as prescribed by the Disclosure of Electronic Data Commission.

The MoPH Notification further clarifies the definition by providing a list of what would constitute health-related personal data which includes, among other things, personal health data (e.g., height, weight, blood type, etc.), medical records, documents and materials relating to personal health data and medical records, etc.

**12. In your jurisdiction, is medical data/healthcare data (e.g. data generated by medical institutions and health care administrative departments in the process of disease prevention and treatment, such as medical records, population health information etc.) more strictly regulated or regulated differently than other types of data? If so, how is medical data/healthcare data defined in your jurisdiction, and how is it regulated?**

In relation to medical records, please see Question 11 above. Under the MoPH Notification, the controller is defined to include government sectors, organizations, hospitals, and other government agencies that would like to jointly use the health-related data which is prepared, gathered, used, or disclosed by the Ministry of Public Health (“Controller”). The Controller is obligated to ensure that the place used for the retention of health-related personal data is in good condition and security measures are implemented.

The MoPH Notification further provides that health-related personal data is confidential and can only be disclosed if consent of the data subject or his/her legal representative has been obtained and as prescribed by law, and such disclosure must not cause damage to the data subject nor the possessor of such data.

**13. Is data related to human genetic resources more strictly regulated or regulated differently than general personal data? If so, how is data related to human genetic resources defined in your jurisdiction, and how is it regulated?**

Data related to human genetic resources are regarded as sensitive personal data under the PDPA and therefore, will be treated the same as other categories of sensitive personal data under the PDPA.

**14. In addition to the above, in your jurisdiction, is there any life sciences & healthcare related data that are regulated differently than data in other sectors? If so, what are these data, and how are they regulated?**

Apart from the above, we are not aware of any life sciences & healthcare related data that are regulated differently than data in other sectors.

# Vietnam

## General questions

1. **Applicable legislation governing data protection in your jurisdiction, for both personal data and non-personal data?**

   *(i) Current Legal Regime*

   The right to privacy and confidentiality of information is a fundamental right recognized by the Constitution of Vietnam. Currently, there is no single comprehensive legal document regulating data privacy in Vietnam. Rather, there are a number of laws relating to personal data privacy, including the following:

   - **Civil Code** (Civil Code No. 91/2015/QH13 adopted by the National Assembly of Vietnam on 24 November 2015 – as amended), effective as of 1 January 2017;
   - **Penal Code** (Penal Code No. 100/2015/QH13 adopted by the National Assembly of Vietnam on 27 November 2015 – as amended), effective as of 1 January 2018;
   - **Cybersecurity Law** (Law on Cybersecurity No. 24/2018/QH14 adopted by the National Assembly of Vietnam on 12 June 2018), effective as of 1 January 2019;
   - **Law on Network Information Security ("LNIS")** (Law on Network Information Security No. 86/2015/QH13 adopted by the National Assembly of Vietnam on 19 November 2015), effective as of 1 July 2016;
   - **Law on Information Technology ("IT Law")** (Law on Information Technology No. 67/2006/QH11 adopted by the National Assembly of Vietnam on 29 June 2006), effective as of 1 January 2007;
   - **Decree 72 on the Internet ("Decree 72")** (Decree No. 72/2013/ND-CP of the Government dated 15 July 2013 on the management, provision and use of internet services and online information – as amended), effective as of 1 September 2013; and
   - **Decree 15 on Handling Administrative Violations in the Fields of ICT and E-Transactions ("Decree 15")** (Decree No. 15/2020/ND-CP of the Government dated 3 February 2020 on handling administrative violations in

the fields of post, telecom, radio frequency, information technology and e-transactions – as amended), effective as of 15 April 2020.

*(ii) Upcoming Draft Legislation*

Two key legal instruments currently in draft form (as of July 2022) will drastically affect the way personal data of individuals in Vietnam is collected and processed, once they officially come into effect:

- **Draft Decree on Personal Data Protection ("Draft PDPD")**: The Draft PDPD has been developed by the Ministry of Public Security of Vietnam (MPS) and is expected to be the very first comprehensive legal instrument governing data protection in Vietnam. Officials have stated that they aim to issue the final PDPD within 2022, but it is difficult to predict when it will actually be issued and take effect.
- **Draft Decree on Implementation of the Cybersecurity Law ("Draft Decree on Cybersecurity")**: This draft decree has been submitted back and forth to the government for review and approval for several years, but there is no official news or certainty as to whether and when the government will issue it.

## 2. Who is/ are the regulator(s) in your jurisdiction for data protection?

As regulations relating to data protection in Vietnam are currently scattered among a number of different legal regimes, various state agencies have authority over data protection, most notably the Ministry of Public Security (MPS) and the Ministry of Information and Communication (MIC).

Once the Draft PDPD comes into effect (assuming no changes are made to the text), a new Personal Data Protection Commission (PDPC) will be established to be the chief regulator for data protection. The PDPC will be directly affiliated with the government, based at the Department of Cybersecurity and Hi-Tech Crime Prevention and Control under the MPS.

## 3. Who are governed by the data protection legislation in your jurisdiction?

In general, the local laws and regulations on data protection apply to any individuals and entities engaging in the collection and processing of data. Given the extremely broad (and sometimes vague) scope of application of these laws and regulations, such individuals and entities would include individuals and entities from both inside and outside of Vietnam.

## 4. Is there an extraterritorial application effect under the data protection legislation in your jurisdiction?

Yes. The relevant laws and regulations apply to individuals and entities from both inside and outside of Vietnam. (See Question 3 above.)

## 5. What are the key aspects to look to when processing personal data in your jurisdiction?

A common key principle under Vietnam's privacy laws is that the collection, storage, use, processing, publication, disclosure and transfer of information and materials related to private life or personal information of an individual must be consented to by that person, unless consent for such transaction is exempted by law (Article 38 of the Civil Code; Article 21 of the IT Law). The law generally does not require a specific form in which consent must be given. It is unclear whether consent must be affirmative or if implied consent is sufficient. However, Vietnam is a very formalistic jurisdiction. Thus, the recommended best practice is clear, affirmative opt-in consent.

The definition of "personal data" under Vietnam's current laws is still scattered among a number of legal instruments. However, the common principle shared by these provisions is that personal data is defined very broadly and generally as any information which can be used to identify a specific person, such as name, age, address, ID card number, telephone number, and email address.

The Draft PDPD sets out the definition of "personal data" in more specific detail. In addition to restating that "personal data" means data about individuals or relating to the identification or ability to identify a particular individual, the Draft PDPD classifies "personal data" into two categories of "basic personal data" (e.g., name, age, address, passport number) and "sensitive personal data" (e.g., personal health data, information on sexual orientation, personal financial data). When the Draft PDPD takes effect, sensitive personal data will be more closely controlled than basic personal data, and the collection and processing of sensitive personal data will require registration with the PDPC.

Furthermore, under the regime of the Draft PDPD, cross-border transfer of personal data outside of Vietnam is also subject to regulatory approval. Specifically, Article 21.1 of the Draft PDPD requires that before transferring Vietnamese citizens' personal data out of Vietnam, the following four conditions must be fulfilled: (i) consent must be obtained from the data subjects; (ii) the original data must be stored in Vietnam; (iii) the data transferor must have proof that the recipient country has personal data protection at a level equal to or higher than the level specified in the Draft PDPD; and (iv) a written approval for transfer must be obtained from the PDPC.

### 6. What are the key aspects to look to when processing non-personal data in your jurisdiction?

Data processors must comply with industry-specific regulations with regard to the processing of non-personal data. However, in general, administrators/operators of information systems which process data have to comply with the following key requirements:

- Administrators of information systems have the responsibility to implement technical measures for preventing acts of cyberattacks from affecting their systems.
- In cases of "cybersecurity emergencies", the organization or individual that detects such emergencies must promptly inform the professional cybersecurity force and implement emergency response measures.

In addition, the illegal collection, exchange, provision, and transfer of any data deemed "state secrets" would be strictly prohibited.

### 7. Is there requirement for data localisation requirement in your jurisdiction?

There is currently no data localization requirement. However, this may change in the near future. In particular, as mentioned above, the Draft PDPD proposes that, before transferring Vietnamese citizens' personal data out of Vietnam, the following four conditions be fulfilled: (i) consent must be obtained from the data subjects; (ii) the original data must be stored in Vietnam; (iii) the data transferor must have proof that the recipient country has personal data protection at a level equal to or higher than the level specified in the Draft; and (iv) a written approval for transfer must be obtained from the PDPC.

However, the foregoing requirements could be exempted if there is: (a) consent from the data subject; (b) approval from the PDPC; (c) a commitment from the data processor to protect the data; and (d) a commitment from the data processor to apply

measures to protect the data. It is still unclear whether one or all of these conditions need to be fulfilled.

In addition, the Law on Cybersecurity requires that domestic or foreign service providers providing services in cyberspace in Vietnam and carrying out activities of collecting, exploiting/using, analyzing, and processing data being personal information, data about service users' relationships and data generated by service users in Vietnam must store such data in Vietnam for a specified period to be stipulated by the government. However, this provision of the law has not yet been enforced, as the MPS is drafting a decree ("Draft Decree on Cybersecurity") to guide the implementation of this data localization requirement.

According to Article 26 of the Draft Decree on Cybersecurity, domestic and foreign enterprises providing telecom and online services to customers in Vietnam could be required to locally store certain customer-related data in Vietnam for a certain period prescribed by law if the authority alerts them that their services/online platforms have been used to commit violations of Vietnam's laws but such online service providers failed to remedy the situation upon the request of the authority.

**8. What are the requirements for cross-border transfer of data in your jurisdiction?**

While Vietnam's current laws only require the data subject's consent for cross-border transfer of personal data, it is required under the Draft PDPD that before transferring personal data of Vietnamese citizens out of Vietnam, a regulatory approval from the PDPC, among other things, must be obtained. For further details, see Questions 5 and 7 above.

# Questions specific to the life sciences & healthcare sector

**9. From the perspective of personal data protection, during the clinical trial of a pharmaceutical/medical device/other types of healthcare products, how is the clinical trial data regulated? Does the general requirements in the questions above apply, or is clinical trial data regulated differently? If not, how is it differently regulated?**

***1) Research data***

*a. Pharmaceuticals*

According to Circular No. 05/2010/TT-BYT of the Ministry of Health dated 1 March 2010, clinical trial data provided in registration dossiers for drugs containing new active ingredients, and meeting the conditions below, must be kept confidential:

(i) It constitutes a trade secret satisfying the protection conditions specified by the Intellectual Property Law;

(ii) It is the result of a substantial investment of efforts; and

(iii) There is a request for confidentiality/security.

When the request is accepted, data security measures will be conducted by the Drug Administration of Vietnam (DAV), including:

(i) Storing and managing documents showing the secured data in accordance with the regulations on confidential document management;

(ii) Not allowing any third party to access the secured data, with the exception of competent agencies' access to verify the clinical trial results, the safety and effectiveness of the drug, or to meet public health protection requirements;

(iii) Not disclosing data, with an exception of necessary disclosure to protect the public.

These measures are applied from the date the data is submitted until the date the data is disclosed, but not exceeding the term stipulated in confidential document management regulations.

Circular No. 29/2018/TT-BYT of the Ministry of Health dated 29 October 2018 further requires researchers and competent management agencies to ensure the confidentiality and integrity of research data. Further, the storage area for relevant records and documents must ensure confidentiality and limited access.

*b. Medical devices*

According to the Regulation on Clinical Trials for Medical Devices (issued together with Decision No. 36/2006/QD-BYT of the Ministry of Health dated 14 November 2006), data subject to preservation and storage includes the clinical trial sheet of the medical device (a document containing records during the course of clinical trials) and relevant documents required for the clinical assessment, figures, original documents, test sheets, relevant collected documents, minutes of meetings of the council, progress reports, research protocols and other documents.

Information relating to the products and product trial results can also be kept confidential.

***2) Participants' personal data***

Participants' personal data is kept confidential according to the Law on Pharmacy and the Regulation on Clinical Trials for Medical Devices. Further, Circular 29 stipulates that the list of trial participants must be encoded/encrypted and then submitted to the management agency after the clinical trial is completed. The retention and submission of the post-encoding list of trial participants must be kept confidential.

The general requirements in the questions above also apply to clinical trial data.

**10. From the perspective of personal data protection, after the pharmaceutical/medical device/other types of healthcare products is marketed, how is the post-marketing data (for example, pharmacovigilance data) regulated? Does the general requirements in the questions above apply? If not, how is it differently regulated?**

According to Article 33 of Decree No. 98/2021/ND-CP of the Government dated 8 November 2021 on medical device management, a medical device registration number holder must establish, organize, and manage the tracing of the origin of the medical device on the market and sufficiently retain all relevant and necessary equipment management records, including the dossier for the issuance of registration number; distribution records; monitoring records of incidents, complaints and remedy measures; and quality management records.

Additionally, according to Article 57.2(b) of the Law on Pharmacy, medicine and medicinal ingredient registration establishments have an obligation to fully retain the

medicine and medicinal ingredient registration dossiers and present them to competent management agencies upon request.

The general requirements in the questions above also apply to the clinical trial data.

**11. In your jurisdiction, is health related personal data related more strictly regulated or regulated differently than other personal data? If so, how personal health data defined in your jurisdiction, and how is it regulated?**

Under the Law on Medical Examination and Treatment, information about the health conditions and private life of patients is required to be kept confidential. However, there are several exceptions where such information can be disclosed:

(i) When the patient consents to the disclosure, or in order to improve the quality of diagnosis, care, and treatment among practitioners directly treating the patient;

(ii) Upon written request for summary information about medical records; and

(iii) With the permission of the head of a medical examination and treatment establishment in the following cases:

- On-premise borrowing in service of research or professional and technical work for internship students, researchers, or practitioners;
- On-premise borrowing in service of an assigned task of authorized entities such as investigation agencies, courts, insurance agencies, and lawyers; and
- Medical record summaries for patients and their representatives.

Those given access to health-related data for approved use must keep it confidential and can only use it exactly pursuant to the purposes proposed with the head of the medical examination and treatment establishment. Particularly for healthcare practitioners, keeping the confidentiality of patients' medical conditions, information that patients have provided, as well as medical records is considered one of the core principles in medical examination and treatment and is also an obligation toward their profession.

In addition, Circular No. 46/2018/TT-BYT of the Ministry of Health dated 28 December 2018 on electronic medical records introduced the deployment of electronic medical records (EMRs) and digitization of medical records nationwide. Each citizen has an electronic health record that is tracked and stored for life. EMRs make it easier to detect any violations of confidentiality of patients' medical records and health data. Article 10 of Circular 46 stipulates that EMR software must be able to track all transactions and user interactions with the software, including the time of viewing, entering, editing, canceling, or restoring data and information in EMRs.

The medical examination and treatment facility itself must also take the following measures:

— Control user access including user authentication, assign user rights according to each role, set time limit allow users to access the software;

— Protect and prevent unauthorized access to EMRs;

— Have a data recovery plan or process in case of failure;

— Have plans to prevent, detect, and remove malware.

In addition, the communication and exchange of EMR data between medical examination and treatment facilities, as well as the patients' medical examination and treatment information, must be encrypted during data exchange according to the instructions of the Minister of Health.

On a related note, according to Article 2.3(b) of the Draft PDPD, personal health data falls within the scope of sensitive data, which requires special consideration and, therefore, stricter regulations than other general personal data. Personal health data is defined as information related to the physical or mental health status of the data subject that is collected or identified during the registration process or the provision of medical services.

In particular, according to Article 8.5 of the Draft PDPD, for the processing of sensitive personal data, the data subject must be provided with an explanation that the data to be processed is sensitive personal data and that the subject's consent must be in a format that can be printed and copied in writing.

Moreover, Article 20.1 of the Draft PDPD requires an organization wishing to collect and/or process sensitive personal data to be registered with the PDPC prior to processing. However, there are certain exceptions in the processing of sensitive data under the Draft PDPD. In particular, the personal data processor is not required to register to process sensitive personal data if the processing aims to serve, among other things, the performance of health care functions of state agencies' health care and social security facilities;

**12. In your jurisdiction, is medical data/healthcare data (e.g. data generated by medical institutions and health care administrative departments in the process of disease prevention and treatment, such as medical records, population health information etc.) more strictly regulated or regulated differently than other types of data? If so, how is medical data/healthcare data defined in your jurisdiction, and how is it regulated?**

Medical/healthcare data is subject to stricter regulations than other types of data. Such data includes the data generated by medical institutions and health care administrative departments in the process of disease prevention and treatment, such as medical records, population health information, etc.

Although Vietnamese law does not clearly define general medical/healthcare data, the law provides the definition of medical records as follows: a case history dossier is a medical, health, and legal record, each patient has only one case history dossier at each time of medical examination and treatment at a medical examination and treatment establishment (Article 59.1 of the Law on Medical Examination and Treatment). In principle, information on the health status and privacy of patients indicated in their case history dossiers must be kept confidential. Such data may be disclosed only when so agreed by patients or for exchange of information and experience between practitioners directly treating the patients to improve the quality of diagnosis, care and treatment of patients or in other cases provided by law.

Article 59.3 further provides measures to preserve medical records. In particular:

(i) Medical records shall be preserved according to the levels of confidentiality under the law on protection of state secrets;

(ii) Medical records of inpatients and outpatients shall be preserved for at least 10 years; medical records of victims of labor and daily-life accidents shall be preserved for at least 15 years; medical records of mental patients and patients who have died shall be preserved for at least 20 years; and

(iii) Medical examination and treatment establishments that preserve case history dossiers electronically shall have backup copies and comply with the above-mentioned regulations.

In addition, please see Question 11 for detailed regulations on EMRs.

Regarding the circumstances in which medical records can be disclosed according to the Law on Medical Examination and Treatment, please also see Question 11.

Since the beginning of 2021, the MOH has been drafting a decree on establishing the legal framework for the construction, management, exploitation and use of a national health database. The draft decree requires the exploitation and use of the national health database to ensure the integrity, privacy, safety and confidentiality of medical information.

**13. Is data related to human genetic resources more strictly regulated or regulated differently than general personal data? If so, how is data related to human genetic resources defined in your jurisdiction, and how is it regulated?**

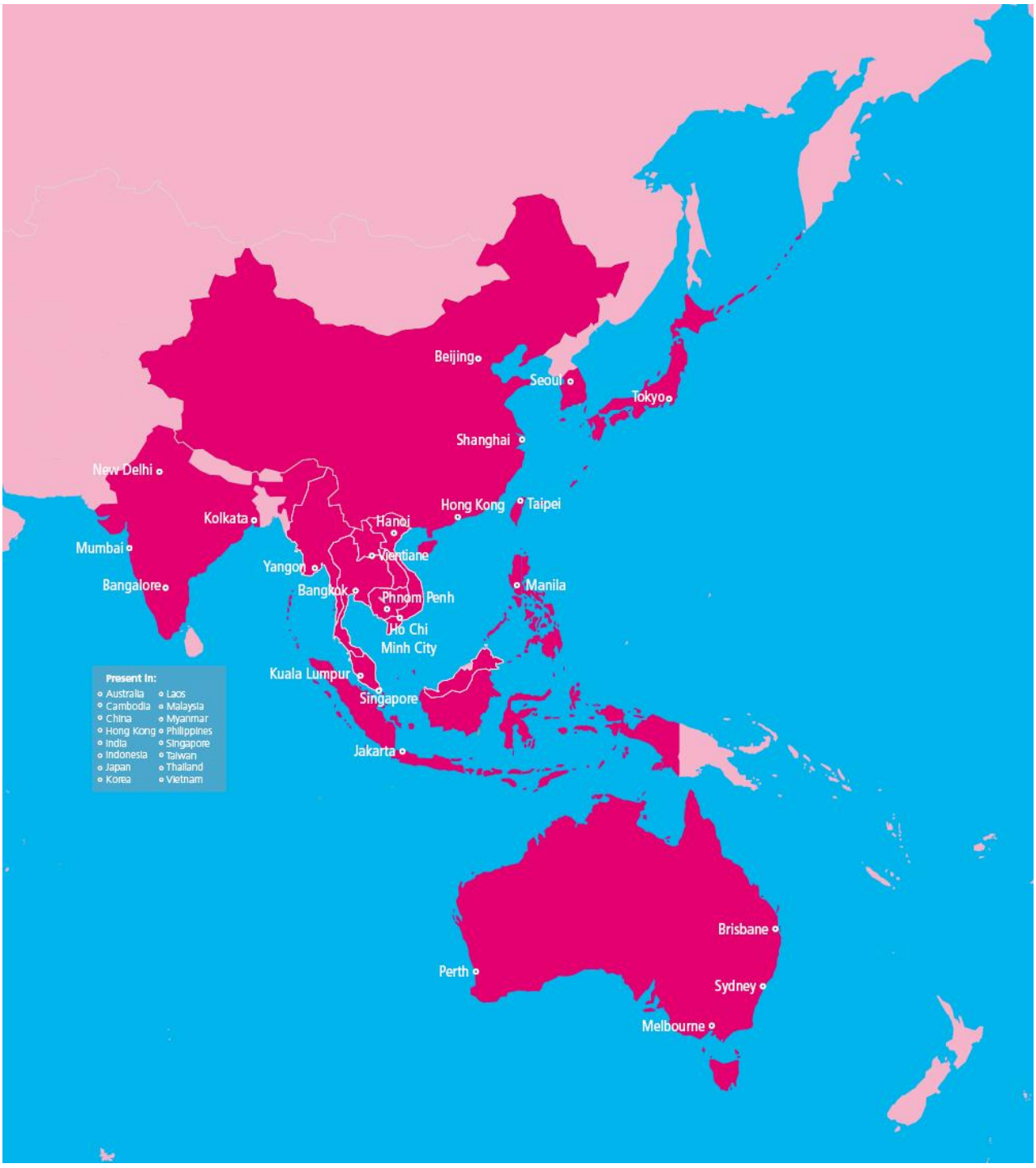
Currently, there are no specific regulations governing human genetic resources. Such data is subject to regulations on general personal data. However, it is worth noting that this may change in the near future. According to Article 2.3(c) of the Draft PDPD, personal genetic data falls within the scope of sensitive personal data and is therefore subject to stricter regulations than general personal data. Personal genetic data is defined as information relating to inherited or acquired genetic characteristics of an individual.

**14. In addition to the above, in your jurisdiction, is there any life sciences & healthcare related data that are regulated differently than data in other sectors? If so, what are these data, and how are they regulated?**

HIV/AIDS-related data is regulated differently from data in other sectors. In particular, Article 8.5 of the Law on HIV/AIDS Prevention and Control prohibits the act of publicizing the name, address, and image of an HIV-infected person or disclosing to others that a person is infected with HIV without that person's consent.

There are certain exceptions to this regulation. In particular, a positive HIV test result can be announced/communicated without the infected person's consent to family members, caretakers, and healthcare workers, among others. These people must keep the test results confidential.

# Locations worldwide



# Contact us

## *Australia*

**Eugenia Kolivos**
Partner
Corrs Chambers Westgarth
**T** +61 2 9210 6316
**E** eugenia.kolivos@corrs.com.au

Eugenia has advised on some of the region's most innovative and cutting edge Intellectual Property projects. With over 20 years' experience in advising on commercial intellectual property in the healthcare and life sciences sectors, she has acted for some of the world's most iconic brands as well as new entrants on research and development activities, partnership and collaboration arrangements, new product and service launches in Australia, healthcare regulatory compliance and consumer law protections.

She also has a wealth of experience in advising on complex IP and IT licensing, distribution and procurement arrangements, technology commercialisation, franchising, outsourcing arrangements and as a service offerings. She has extensive experience in drafting and negotiating transitional service arrangements as part of corporate restructures as well as ongoing supply agreements.

Eugenia has extensive experience in advising on privacy and data protection issues in Australia, including the intersection of privacy laws with personal information used in the implementation and roll-out of digital healthcare services, medical devices and other therapeutic goods and services.

Eugenia has developed a reputation as a lawyer that understands the commercial imperatives, working to provide practical and workable business solutions. She has been praised for never acting as a "handbrake" for business, highly responsive and always working to ensure that business outcomes are achieved in a compliant and practical manner.

Eugenia is consistently listed as a leading lawyer by legal directories and publications including Chambers and Partners, Best Lawyers, Legal 500 and World Trade Mark Review.

## *China/Hong Kong*

**Nick Beckett**
Managing Partner, Beijing and Hong Kong Offices
Global Co-Head CMS Life Sciences & Healthcare Sector Group
**T** +86 10 8527 0287/+852 2533 7818
**E** nick.beckett@cms-cmno.com

Nick is the Managing Partner of the Beijing and Hong Kong Offices, Global Co-Head of CMS Life Sciences & Healthcare Sector Group and Head of Asia-Pacific IP. Nick is also a registered foreign lawyer in Hong Kong. Nick has extensive experience in advising on all aspects of intellectual property, regulatory and commercial matters affecting Life Sciences & Healthcare clients internationally and his practice spans both contentious and non-contentious issues.

Nick has substantial experience in coordinating complex multi-jurisdictional matters, regularly working with colleagues throughout CMS and around the world. His work in the areas of commercial and corporate transactions and disputes, parallel trade, anti-counterfeiting, trade mark and patent opinions and IP infringement particularly spans international borders.

Nick is recommended as a prominent practitioner in his field in Chambers & Partners, Legal 500, Euromoney's Expert Legal Guide – Life Sciences, Who's Who Legal Life Sciences (Patent Litigation, Regulatory, Transactional), IAM 1000 and Who's Who Legal: *Thought Leaders – Global Elite for Life Sciences*. Nick is also recommended in Who's Who Legal 'China – Patents and Life Sciences'. Nick was awarded '*Life Sciences Lawyer of the Year in China'* in Leaders in Law - 2020 Global Awards, The Best Lawyers in China 2020 for Intellectual Property Law (International Firms).

Nick has also been recognised as a *'Top 15 IP Lawyer in China'* by Asian Legal Business 2017, *IP (Expertise Based Abroad) - UK* in Chambers Global.

Nick led the team on Takeda's €9.6 billion acquisition of Swiss drug company, Nycomed A/S, which won the FT & Mergermarket Private Equity's Deal of the Year. In China, Nick's team has been ranked in the Asian Legal Business Asia's Top 50 Largest Law Firms (2014-2021) and been highly commended at the FT Innovative Lawyers for Asia-Pacific (2014-2020). In addition, the IP team in Asia is recognised in the Asian Legal Business IP Rankings.

Nick is a Solicitor-Advocate of the English Courts and a listed Arbitrator at the Beijing International Arbitration Centre (BIAC) and Beijing Arbitration Commission (BAC) and an 'Advisory Expert of the National Advisory Center for Overseas Intellectual Property Dispute Settlement' in China. He is an Honorary Lecturer at the China Pharmaceutical University in Nanjing and lectures also at Peking University, University of International Business and Economics (UIBE) and China-EU School of Law at China University of Political Science and Law.

## *Indonesia*

**Eko Basyuni**
Partner
Assegaf Hamzah & Partners
**T** +62 21 2555 7802
**E** eko.basyuni@ahp.co.id

Eko holds an LL.M. in banking and financial law from Boston University and has more than 15 years' experience as a legal practitioner. His focus extends across the corporate, banking & finance, and FDI practices, and he has amassed extensive experience in a range of rapidly expanding sectors, including Lifesciences, the creative industries and TMT.

He has advised a number of multinational companies on their FDI ventures in Indonesia, and is an Asialaw Profiles 'Recommended Lawyer.' His expertise was one of the contributing factors to Assegaf Hamzah being named an Asian-Mena Counsel 2014 'In-house Community Firm of the Year' in Indonesia for Lifesciences.

Prior to joining Assegaf Hamzah, Eko served as legal counsel with the Indonesian Bank Restructuring Agency (IBRA) during a tumultuous period that saw the agency rebuild the country's decimated financial services sector from the ruins of the 1997/98 Asian financial crisis. Eko speaks Indonesian and English.

## *Japan*

**Chie Kasahara**
Partner
Atsumi & Sakai
**T** +81 3-5501-2438
**E** chie.kasahara@aplaw.jp

Chie, a Japanese-qualified attorney (Bengoshi) of some 15 years' standing, leads the IP/IT & Healthcare team. She is an IP/IT & Healthcare practitioner with deep knowledge of legal issues relevant to the lifesciences field, and highly experienced in patent and regulatory/compliance matters. She represents biotechnology, medical device and other pharmaceutical companies in patent protection and litigation both domestic and cross-border. She also advises her clients on licensing, transfer, development and collaboration agreements.

## Korea

**Ki Young Kim**
Partner
Yulchon LLC
**T** +82 2 528 5222
**E** kykim@yulchon.com

Ki Young is a co-chair of Yulchon's Healthcare Practice Team and a partner in the Corporate & Finance Group. After joining Yulchon in 1998, he successfully advised a number of international and Korean pharma/medical device companies on general corporate matters, including mergers and acquisitions, joint ventures and other strategic alliances, drug/medical device sales and distribution agreements, R&D related matters, and licensing and related disputes. Ki Young also specializes in government regulation and policy issues, including issues related to product approvals, market access, pricing, labeling, advertisement, healthcare insurance and regulation by the MOHW and the MFDS. Ki Young also provides extensive compliance and anti-corruption advice related to marketing activities to numerous international and Korean pharma/ medical device companies.

Ki Young's experience includes a secondment with Allen & Overy, Hong Kong from 2003 to 2004 and service as an outside director of Ildong Pharmaceutical Co., Ltd. from 2010 to 2014. Currently, he serves as a legal adviser to the Korean Cosmetics Association, Korea Pharmaceutical Traders Association and Korea Medical Devices Industry Association, and he is an IRB member of St. Mary Hospital in Seoul.

Ki Young speaks English and Korean.

## Singapore/Malaysia/Philippines

**Wee Hann Lim**
Partner
Rajah & Tann Singapore LLP
**T** +65 6232 0606
**E** wee.hann.lim@rajahtann.com

Wee Hann has over 23 years of experience in advising companies on cross-border investments, private mergers & acquisitions, sale & purchase of companies and businesses and other corporate transactions. Wee Hann also specialises in labour law and employee benefits.

Wee Hann's expertise includes advising numerous biotechnology, health and pharmaceutical global leaders on cross-border acquisitions and divestments. He is a recommended lawyer in the PLC Lifesciences Handbook for his work in the Lifesciences industry and is also listed by the International Who's Who of Lifesciences Lawyers as one of the world's leading practitioners in the field of Lifesciences.

Wee Hann speaks English, Bahasa Malaysia, Mandarin, Vietnamese and is learning Japanese.

## Taiwan

**Jennifer Wang**
Partner
Chen & Lin Attorneys-at-Law
**T** +886 2 2715 0270
**E** jenniferwang@chenandlin.com

Jennifer is the partner of Chen & Lin Attorneys-at-Law since 2008. Jennifer and Chen & Lin team have extensive experiences in serving clients in the sector of pharmaceuticals, biotech, medical device, nutritious food as well as cosmetics, including both domestic and international companies, hospitals, laboratories, associations and individuals.

Jennifer's specialised legal areas include foreign (PRC) investment, legal compliance, corporate, M&A, securities and anti-trust related issues. Jennifer, together with the team, provides holistic legal services to Lifesciences clients, ranging from administrative application, local legal compliance, fundraising, M&A, IPO, licensing, daily

operation related agreements, patent litigation, maltreatment litigation and criminal procedures about health insurance fraud. Jennifer is one of the ranked lawyers in Taiwan in Chambers & Partners Asia-Pacific 2018 in the fields of corporate/M&A and capital market.

Jennifer speaks Mandarin and English.

## *Thailand/Cambodia/Laos/Myanmar*

**Alan Adcock**
Partner
Tilleke & Gibbins
**T** +66 2056 5871
**E** alan.a@tilleke.com

Alan is a partner in the Tilleke & Gibbins' intellectual property and regulatory affairs groups, helping to oversee the firm's client work in these areas across ASEAN. He also co-heads the firm's regional lifesciences practice with Thomas Treutler.

Alan has over 20 years' experience in Asia, during which time he has devoted much of his work to IP acquisitions, strategic structuring, technology transfer, and IP licensing and securitisation agreements, mainly in the pharmaceutical, agrochemical, and material science sectors. He handles various IP infringement and regulatory infraction cases involving labelling, advertising, clinical trials, product handling/warehousing, product registration, taxation, and import/ export violations in the Asia-Pacific region. He also deals with local pre-litigation strategy and litigation management for infringement and invalidation matters in the region.

Since 2005, Alan has been recognized by *Asialaw Leading Lawyers* as one of Asia's leading business lawyers in the area of intellectual property, and he has been named a top IP lawyer in Thailand by *The Legal 500 Asia Pacific* and *WTR 1000*. Alan is also recognized as a leading IP strategist by *IAM Strategy 300*, an expert on patents in *IAM Patent 1000*, one of the world's foremost lifesciences practitioners by *IAM Lifesciences 250*, and a leading lifesciences regulatory lawyer by *Who's Who Legal*.

Alan is licensed to practice in New York and New Jersey and is admitted in the U.S. District Courts of Southern and Eastern New York. He speaks English and Mandarin.

## *Vietnam*

**Thomas J. Treutler**
Partner
Tilleke & Gibbins
**T** +84 8 3936 2068
**E** thomas.t@tilleke.com

Tom is the Managing Director of Tilleke & Gibbins' Vietnam offices. He is an attorney licensed by the State Bar of California and is registered to practice as a foreign lawyer in Vietnam and before the USPTO and the U.S. Court of International Trade.

Tom has worked in the legal services field in Vietnam since 1994, specializing in corporate and commercial law as well as IP. He co-heads Tilleke & Gibbins' regional lifesciences practice with Alan Adcock. Recognized as a leading lawyer by *Chambers*, *The Legal 500*, and *Managing IP*, Tom has extensive experience in IP enforcement and has secured a number of landmark victories for foreign investors operating in the lifesciences and technology sectors.

Tom is a former Chair of the East Asia and Pacific Subcommittee of INTA's Famous and Well-Known Marks Committee, is a member of the INTA Asia-Pacific Global Advisory Council, and currently sits on the INTA Copyright Academic Committee. He has advised EuroCham Vietnam's Pharma Group (an industry group of major pharmaceutical innovators), and has assisted with drafting position papers on compulsory licensing and a roadmap for Vietnam's compliance with the EU-Vietnam Free Trade Agreement and TRIPS. Tom also serves as a local expert for Vietnam for the European Commission's ASEAN IPR SME Helpdesk.

Tom earned his JD, *magna cum laude*, from Indiana University Bloomington's Maurer School of Law, where he now serves as a member of the Dean's Global Advisory Board. He speaks English and Vietnamese.

The collaboration presented in this publication is limited to Lifesciences. The information held in this publication is for general purposes and guidance only and does not purport to constitute legal or professional advice.

Assegaf Hamzah & Partners, Atsumi & Sakai, Chen & Lin, CMS, China, Corrs Chambers Westgarth, Rajah & Tann Singapore LLP, Tilleke & Gibbins and Yulchon LLC are all independent law firms.

Further information about each firm can be found respectively at www.ahp.co.id, www.aplaw.jp/en/, www.chenandlin.com, cms.law, www.corrs.com.au, www.rajahtann.com, www.tilleke.com, www.yulchon.com