Baker McKenzie.

2024 Asia Pacific Guide for Insurance Data Protection and Cybersecurity

Click here to enter Subtitle.

Foreword

Data privacy and cybersecurity are topics that continue to be of interest to many industry players. This is due to the increased implementation and management of global databases, outsourcing, litigation, and internal investigation and crisis management concerns, all of which trigger a variety of privacy and security compliance issues. The way in which data is being used is also evolving — insurers are exploring the monetization of data sources and deploying new technologies such as blockchain, artificial intelligence and Internet of Things (IoT), which may impact how data security is managed.

Although much of the regulatory focus has been on data protection and privacy in the region, notorious cyber attacks on financial institutions have incentivized regulators to set standards on risk identification, assessment, mitigation, and crisis management. At this stage, the regulatory landscape remains fragmented. Each country in Asia Pacific has prescribed requirements with local nuances. The practicality and level of enforcement differs from one country to another.

While the innovation of the insurance industry in embracing insurtech has harnessed new market opportunities and increased growth, it has also had an impact on internal core processes, which radically increase the risk of data security breaches. Utilization of social media platforms to enhance service offerings also adds to this risk. Controversies surrounding the wider range of non-traditional data and related analytics are anticipated to increase.

Table of contents

Regulatory environment

1. Who is the main regulator with oversight of data privacy matters?

China	The Cybersecurity Administration of China (CAC) is responsible for the overall coordination, supervision and administration of personal information protection and cyber data security work. The Ministry of Public Security (MPS) and the Ministry of Industry and Information Technology (MIIT), together with relevant industrial regulators (in the case of insurance companies, the National Administration of Financial Regulation or NAFR), will likely take the lead in enforcing the compliance requirements on data privacy.
Hong Kong	The Office of the Privacy Commissioner for Personal Data (PCPD)
Indonesia	There is not yet a specific data privacy regulator in Indonesia. The Ministry of Communication and Informatics (MOCI) has overall responsibility for data privacy, and the government authority for financial institutions (including insurance companies) is the Financial Services Authority (OJK). Note that the government will stipulate a Data Protection Authority based on the PDP Law.
Japan	The Personal Information Protection Commission (PPC)
Malaysia	The Personal Data Protection Commissioner (Regulator)
Philippines	The National Privacy Commission (NPC) is the regulatory agency tasked to administer the Philippines' Data Privacy Act of 2012 (DPA). Data-privacy-related regulations of the Philippine Insurance Code and regulations issued by the Philippine Insurance Commission (IC) are administered by the IC.
Singapore	The Personal Data Protection Commission (PDPC)
Taiwan	Currently, the Insurance Bureau (IB), Financial Supervisory Commission (FSC) is the personal data protection regulator for insurance enterprises. In May 2023, Taiwan legislators amended Article 1-1 of the Personal Data Protection Law, which designates the new Taiwan Personal Data Protection Commission (Taiwan PDPC) as the competent authority for personal data protection. As of May 2024, the effective date of the amendment to Article 1-1 of the Personal Data Protection Law has not yet been decided. The preparatory office for the Taiwan PDPC was established on 5 December 2023, and the Taiwan PDPC is expected to be established by August 2025. From the date of the Taiwan PDPC's establishment, it will be the coordinating independent supervision agency tasked to administer the Personal Data Protection Law. However, the insurer enterprises' security maintenance plan for the files of personal data and the processing of personal data after the termination of business with the data subject will still be governed by the IB and FSC after the establishment of the Taiwan PDPC.
Thailand	The Personal Data Protection Committee (PDP Committee)
Vietnam	Multiple government agencies have overlapping oversight power. Those agencies include the Ministry of Public Security (MPS), which is the main enforcer of the newly issued Decree No. 13/2023/ND-CP on Personal Data Protection (PDPD); the Ministry of Information and Communications (MIC), which is the main enforcer of the cyber information security laws; and other relevant agencies in specific sectors (e.g., banking and finance, trade and consumer protection).

2. What is the main legislation on the protection of personal data privacy?

China	The main legislations are the Personal Information Protection Law (PIPL), which took effect in November 2021, and the Data Security Law (DSL), which took effect in September 2021. In addition to the PIPL and the DSL, there are various regulations and standards for different industries. The regulations and standards that apply to the insurance sector mainly include the Personal Financial Information Protection Technical Specification (JR/T 0171—2020), the Draft Internet Insurance Business Regulation published in 2020, the Measures for the Administration of the Protection of Consumer Rights and Interests by Banking and Insurance Institutions published in 2022, and the Draft Measures for the Management of Banking and Insurance Supervision Statistics published in 2022, among others.
Hong Kong	Personal Data (Privacy) Ordinance (Cap. 486) (PDPO)
Indonesia	The main regulation is Law No. 27 of 2022 on Personal Data Protection (PDP Law), the Ministry of Communication Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems (Regulation 20), as well as the provisions under Law No. 11 of 2008 on Electronic Information and Transaction, as lastly amended by Law No. 1 of 2024 (EIT Law) and its implementing regulations. Insurance companies are also subject to regulations issued by the OJK, such as OJK Circular Letter No. 14 of 2014 on Confidentiality and Security of Customers' Private Information and OJK Regulation No. 1 of 2013 on Protection for Financial Services Consumers.
Japan	The main legislation is the Act on Protection of Personal Information (Act No. 57 of 30 May 2003) (APPI). The Guidelines for the Act on Protection of Personal Information (PPC Notices No. 6-9 of 2016) function as general guidelines (Guidelines). In addition to the APPI and the Guidelines, there are some industry-specific guidelines issued by different Japanese government agencies. The guidelines that apply to the insurance sector are the Guidelines for Personal Information Protection in the Financial Sector (PPC and FSA Notice No. 1 of 28 February 2017) and the Practical Guidelines for Security Control Measures Provided in the Guidelines for Personal Information Protection in the Financial Sector (PPC and FSA Notice No. 2 of 28 February 2017) (collectively, PPC and FSA Guidelines).
Malaysia	The Personal Data Protection Act 2010 (PDPA); the Code of Practice on Personal Data Protection for the Insurance and Takaful Industry in Malaysia (Code), which came into effect on 23 December 2016, should be read together with the PDPA.
Philippines	Republic Act No. 10173 or the DPA, which took effect on 8 September 2012, and its implementing rules and regulations (DPA IRR), which took effect on 9 September 2016, govern personal data protection in the Philippines.
Singapore	The Personal Data Protection Act 2012 (PDPA) and subsidiary legislation such as the following: Personal Data Protection (Appeal) Regulations 2021; Personal Data Protection (Composition of Offences) Regulations 2021; Personal Data Protection (Do Not Call Registry) Regulations 2013; Personal Data Protection (Enforcement) Regulations 2021; Personal Data Protection (Notification of Data Breaches) Regulations 2021; Personal Data Protection (Prescribed Healthcare Bodies) Notification 2015; Personal Data Protection (Prescribed Law Enforcement Agencies) Notification 2014; Personal Data Protection (Prescribed Law

		Enforcement Agency) Notification 2020; Personal Data Protection (Statutory Bodies) Notification 2013 and Personal Data Protection Regulations 2021
	**Taiwan**	The Personal Data Protection Law (PDPL)
	**Thailand**	The Personal Data Protection Act 2019 (PDPA) , as well as its subordinate regulations
	**Vietnam**	Decree No. 13/2023/ND-CP on Personal Data Protection (PDPD) Despite the enactment of this comprehensive legal regime, data protection regulations remain scattered in various other pieces of legislation that are still in force, some of which can prevail over the PDPD in case of inconsistencies (e.g., Law on Protection of Consumer's Rights), given the hierarchy of legal documents under the Vietnamese legal system.

3. Who is the main regulator with oversight of cybersecurity matters?

China	CAC, MPS and MIIT
Hong Kong	There is no specific regulator. For insurance companies, the Insurance Authority remains the main regulator.
Indonesia	The MOCI and the National Code and Cyber Agency (Badan Sandi dan Siber Negara or BSSN)
Japan	The Cybersecurity Strategic Headquarters and the National Center of Incident Readiness and Strategy for Cybersecurity
Malaysia	The Malaysian Communications and Multimedia Commission and CyberSecurity Malaysia
Philippines	The Office of Cybercrime (OCC) under the Department of Justice coordinates the law enforcement efforts of the government against cybercrime and assists in the prosecution of cybercrimes. The OCC implements the Cybercrime Prevention Act of 2012 (Anti-Cybercrime Law). On the other hand, the Department of Information and Communications Technology (DICT) is the primary policy, planning, coordinating, implementing and administrative entity of the government that plans, develops and promotes the national information and communications technology (ICT) development agenda.
Singapore	The Cyber Security Agency of Singapore (CSA)
Taiwan	The Ministry of Justice and the Administration for Cyber Security of the Ministry of Digital Affairs
Thailand	The National Cyber Security Committee (NCSC)
Vietnam	Cybersecurity matters (i.e., assurance that activities in cyberspace shall not interfere with national security, social order/safety and legitimate rights of organizations/individuals) are jointly regulated by the Ministry of Public Security (MPS), the Ministry of National Defence, and the Government Cipher Committee under the Ministry of Defence (GCC). Cyber information security matters (i.e., prevention of illegal use or intrusion of the information system in cyberspace) are regulated by the MIC.

4. Is there existing legislation governing cyber security issues?

China	In addition to the Cybersecurity Law that came into effect on 1 June 2017, other implementation regulations, rules and guidelines in accordance with the Cybersecurity Law include the Draft Implementation Opinions on Carrying Out Certification of Network Security Services issued in 2023, the Measures for Cybersecurity Review taking effect in 2022, the Regulation on Protecting the Security of Critical Information Infrastructure taking effect in 2021, and the Guiding Opinions on Strengthening Industrial Internet Security issued in 2019, among others.
Hong Kong	There is no specific legislation governing cybersecurity. However, the Insurance Authority has issued a Guideline on Cybersecurity (GL20), which came into effect on 1 January 2020.
Indonesia	There is no specific regulation on cybersecurity in Indonesia. The EIT Law and its implementing regulation, Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions (GR 71), are the main legislation that cover general provisions on cybersecurity.
Japan	The Basic Act on Cybersecurity provides the framework of the government's cybersecurity strategy and its basic policies.
Malaysia	Aside from the PDPA, these are the Computer Crimes Act 1997, Electronic Commerce Act 2006, and the Communications and Multimedia Act 1998. The Malaysian Parliament has recently passed the Cyber Security Bill, which is expected to serve as the overarching cyber security legislation. It has yet to come into force. The Central Bank of Malaysia (BNM) has issued the Risk Management in Technology (RMIT) policy document and the Management of Customer Information and Permitted Disclosures policy document, which are specific to financial institutions (such as insurers) and which require these financial institutions to comply with additional cybersecurity requirements.
Philippines	In addition to the DPA and DPA IRR, the Anti-Cybercrime Law (Republic Act No. 10175), which took effect on 12 September 2012, and its implementing rules and regulations (Cybercrime Law IRR), which took effect in 2015, govern cybersecurity issues in the Philippines. The DICT has also issued policies on ICT and cybersecurity.
Singapore	The Computer Misuse Act 1993 and subsidiary legislation such as the Computer Misuse (Composition of Offences) Regulations The Cybersecurity Act 2018 and subsidiary legislation such as the Cybersecurity (Composition of Offences) Regulations 2022; Cybersecurity (Confidential Treatment of Information) Regulations 2018; Cybersecurity (Critical Information Infrastructure) Regulations 2018; and Cybersecurity (Cybersecurity Service Providers) Regulations 2022 The Cybersecurity (Amendment) Bill, amending the Cybersecurity Act, was just passed on 8 May 2024, but there is no visibility on when the revised Cybersecurity Act will come into force.
Taiwan	Cyber Security Management Act and the implementation regulations, rules and guidelines issued in accordance with the Cyber Security Management Act (e.g., the Operational Measures for the Cyber Security Management of Specific Non-Governmental Agencies under the Administration of the Financial Supervisory Commission applicable to financial institutions including the insurance companies) Aside from the above cyber security management regulations and the PDPL, Chapter 36 of the Criminal Code also has provisions regarding computer security

		offenses. In Chapter 28 of the Criminal Code, there are provisions in connection with using computers to commit offenses against privacy.
	**Thailand**	Cybersecurity Act 2019 (Cybersecurity Act), which is the first legislation to govern cybersecurity in Thailand
	**Vietnam**	Cybersecurity issues are mainly regulated under the Law on Cyber Information Security, Cybersecurity Law, and their implementing regulations.

Technology and risk management

5. What are the main requirements with respect to collection, use, disclosure or transfer of personal data?

China

An insurer (i.e., a data user) that processes personal data should comply with the following requirements set out by the PIPL:

- Main principles of collecting and processing personal data - Personal data shall be processed under the principles of lawfulness, legitimacy, necessity and good faith; personal data processing shall be for a clear and reasonable purpose, directly related to the processing purpose and in a manner that has the minimum impact on the rights and interests of individuals; and personal data shall be processed under the principles of openness and transparency.
- Consent - The entity collecting personal data should explicitly inform the data subjects of the purposes, scope and manner of data collection, and use (including transfer of data to overseas) and obtain the data subjects' consent to the same. In the case of any change of the purpose or method of processing of personal data, or the category of personal data to be processed, the individual's consent shall be obtained anew. The legal custodians' consent for the collection, use, transfer and disclosure of personal data of children under 14 must also be obtained.
- Retention of personal data - A retention period of personal data shall be the shortest time necessary to achieve the processing purpose, except as otherwise provided by any law or administrative regulation.
- Disclosure of personal data - The entity processing personal data shall not disclose the personal information processed, except with the separate consent of the individuals.
- Transfer of personal data - The entity processing personal data that provides any other personal data processor with the personal data it processes shall notify individuals of the recipient's name, contact information, purposes and methods of processing, and categories of personal information, and obtain the individuals' separate consent.
- Offshore data transfer - If the entity collecting personal data is an operator of critical information infrastructure (likely to include any insurance company licensed in China), personal data collected or generated in China must be stored and processed within China, and provision of the same to overseas entities will be subject to a security assessment conducted by Chinese regulators.

Hong Kong

An insurer (i.e., a data user) handling personal data should follow the six data protection principles (DPPs) below:

- Purpose and manner of collection of personal data - The purpose of collection of personal data must relate to a function of the data user. Collection of the data should be necessary for or directly related to that purpose, and the data collected should not be excessive. The means of collection must be lawful and fair.
- Accuracy and duration of retention of personal data - A data user must take all practicable steps to ensure the accuracy of personal data it holds and to erase the data after fulfilment of the purposes for which the data is used.

	▪ Use of personal data - Unless prior 'prescribed consent' has been obtained from the data subject (e.g., the customers), personal data shall not be used for a new purpose. ▪ Security of personal data - A data user must take all practicable steps to ensure that the personal data it holds is protected against unauthorized or accidental access, processing, erasure or other use. ▪ Information to be generally available - A data user must take all practicable steps to ensure openness and transparency about its policies and practices in relation to personal data. ▪ Access to personal data - A data user is required to comply with requests from data subjects for access to and correction of personal data it maintains.
Indonesia	▪ Lawful basis - Data controllers must have a lawful basis to collect, use and process personal data. There are six lawful bases that are recognized in Indonesia based on the PDP Law: consent, implementation of contracts, fulfilment of legal obligation, protection of vital interest, implementation of public services, and fulfilment of legitimate interest. ▪ System certification - Electronic system operators must use a certified electronic system. ▪ Collection and utilization of personal data - The collection and utilization of personal data are limited for the specific purposes set out in the consents provided by the data owners. ▪ Offshore data transfer - Offshore data transfers may only be conducted if one of the following requirements is met: (i) the nation where the receiving party is located has a similar or the same standard of personal data protection as the PDP Law; (ii) there is a sufficient and binding data protection provisions; or (iii) there is consent from the data subject. ▪ Data breach - Data controllers are required to promptly notify the data owners in writing when there is a data breach. The notification must be done within 72 hours. ▪ Right to be forgotten - The data owner has the right to request their personal data to be removed at any time. The deletion must be made in accordance with the prevailing laws and regulations (e.g., the deletion is being made based on a court order). The right to be forgotten also includes delisting of the relevant information from search engine results. ▪ Data protection officer - Data controllers and data processors that meet certain thresholds must appoint a data protection officer. ▪ Data Privacy Impact Assessment - Data controllers that conduct 'high-risk' processing activities must conduct a DPIA.
Japan	▪ Purpose of use of personal information - 'Purpose of use' refers to the business operators' intended use for the personal information. Such purpose of use needs to be as specific as possible. ▪ Manner of collection of personal information - Once the business operator has acquired personal information, it must promptly notify the data subject of, or publicly announce, the purpose of use of such personal information, unless it has already publicly announced its purpose of use. ▪ Use of personal data - Any use of the personal information by the business operator must be made within the scope of the purpose of use. A data subject's prior consent is required for the transfer of personal data, unless the exceptions provided in the APPI are applicable. Under the amended APPI, there are also

record-keeping requirements on business operators that transfer or receive personal data.

- Security of personal data - The APPI states that business operators must: (a) take necessary and appropriate measures to prevent leakage, loss or damage of personal data, and otherwise ensure proper security management of personal data; and (b) exercise necessary and appropriate supervision over the subcontractor to ensure proper data security management.
- Cross-border disclosure of personal information -Transfer of personal data to a recipient outside Japan requires either: (i) the data subject's informed consent; (ii) appropriate safeguards for protection of the personal data (e.g., having in place a data transfer agreement with the recipient); or (iii) the PPC's adequacy decision recognizing the data protection laws in the recipient's jurisdiction provides sufficient protection for the personal data.
- Accuracy of personal data - The APPI encourages business operators to maintain accurate and up-to-date personal data within the scope necessary to achieve the purpose of use.
- Access to personal data - The personal data processed by the business operators must be disclosed to the data subjects upon request. If data subjects request disclosure of or modifications to their information, the business operator must, in principle, comply with such requests unless exempted under the APPI.

Malaysia

An insurer (i.e., a data user) that processes personal data should comply with seven data protection principles pursuant to the PDPA, as discussed further below. The term 'processing' is defined very broadly to include, among others, collecting, recording, holding, storing, disclosure and transfer of personal data.

- General principle - Processing of personal data requires consent from data subjects.
- Notice and choice principle - Data users are required to notify data subjects in writing of a number of prescribed matters, including, but not limited to, the purpose for which the data is collected and the right to request access and correction of personal data (Prescribed Matters).
- Disclosure principle - No personal data shall be disclosed without the consent of the data subjects.
- Security principle - A data user shall take practical steps to protect personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration, or destruction.
- Retention principle - Personal data processed for any purpose shall not be kept longer than is necessary for the fulfilment of that purpose.
- Data integrity principle - A data user shall take reasonable steps to ensure that personal data is accurate and up to date.
- Access principle - Data subjects shall be given access to their personal data and shall be able to correct inaccurate or incomplete data.

An insurer will also have to comply with the requirements of the Code. The Code expands on the seven data protection principles as it relates to the conduct of insurers specifically. For example, the Code provides the circumstances in which a customer has been deemed to have given their consent for the processing of their personal data.

These general obligations are overlaid with the need for insurers to comply with the specific requirements imposed by BNM in connection with the handling of data and customer information. These specific requirements include, among others, the following:

- Establishing written policies and procedures to safeguard customer information, which covers collection, storage, use, transmission, sharing, disclosure and disposal of customer information
- Restricting the ability to download customer information in portable storage devices provided by the insurer to employees with a legitimate business, and ensuring that such devices are adequately protected by relevant controls
- Reviewing access rights and immediately revoking access rights of an employee leaving the insurer or moving to a new role that does not require access to customer information
- Establishing mechanisms that create a strong deterrent effect against unauthorized disclosure by whatever means of customer information by employees.

Philippines

Under Section 1 (o) of the DPA, any operation or any set of operations performed upon personal data, including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data, is considered 'processing' of personal information. Processing may be performed through automated means or manual processing if the personal data are contained or are intended to be contained in a filing system. Unless there is a specific law that otherwise prohibits the processing of personal information under particular circumstances, the processing of personal information is allowed when at least one of the conditions below exists:

- There is consent from the data subject (which must be given prior to the collection of such personal information, or as soon as practicable and reasonable).
- The processing involves the personal information of a data subject who is a party to a contractual agreement, in order to fulfil obligations under such contract, or in order to take steps prior to entering into said contract at the request of the data subject.
- The processing is necessary for compliance with a legal obligation of the personal information controller (PIC), or the person/organization who/which controls the collection, holding, processing or use of personal information, including those who/which instructs another to collect, hold, process, use, transfer or disclose personal information on its/their behalf.
- The processing is necessary to protect vitally important interests of the data subject (e.g., life and health).
- The processing of personal information is necessary to respond to national emergencies, or to comply with the requirements of public order and safety, or to fulfil a function of public authority.
- The processing is necessary to pursue the legitimate interests of the PIC or by the third party(ies) to whom the information is disclosed, subject to the protection of fundamental rights and freedoms of the data subject under the Philippine Constitution.
- There are separate rules and legal bases for the processing of sensitive personal information (see item 7). As a general rule, consent of the data subject is required to process sensitive personal information.

Moreover, in principle, the processing of personal and sensitive personal information must comply with the three basic principles of transparency, legitimacy of purpose and proportionality.

- Transparency - The processing must be transparent, such that the data subject must be made aware at the onset, through plain and clear language, of the nature, purpose and extent of the processing of their personal data, including

the risks and safeguards involved, their rights as data subject, and how these rights can be exercised.

- Legitimacy - The processing must be made for a legitimate purpose, such that the same is compatible with the declared and specified purpose, which is not contrary to law, morals or public policy.
- Proportionality - The processing must be proportional to the declared and specified purpose, and not overly excessive.

Singapore

Organizations are required to comply with the following 10 key obligations under the PDPA:

- Consent - Collect, use or disclose personal data for purposes for which an individual has given. Allow individuals to withdraw consent, with reasonable notice, and inform them of the likely consequences of withdrawal. Upon withdrawal of consent, cease such collection, use or disclosure of personal data.
- Purpose - Collect, use or disclose personal data about an individual for purposes that a reasonable person would consider appropriate in the circumstances and for which the individual has given consent.
- Notification - Notify individuals of the purposes for which the organization intends to collect, use or disclose their personal data on or before such collection, use or disclosure of personal data.
- Access and correction - Upon request, the personal data of an individual and information about the ways in which their personal data may have been used or disclosed in the past year should be provided. It is also a requirement to correct any error or omission in an individual's personal data upon their request.
- Accuracy - Make reasonable efforts to ensure that personal data collected by or on behalf of the organization is accurate and complete if it is likely to be used to make a decision that affects the individual or if it is likely to be disclosed to another organization.
- Protection - Make reasonable security arrangements to protect the personal data that you possess or control to prevent unauthorized access, collection, use, disclosure or similar risks.
- Retention limitation - Cease retention of personal data or remove the means by which the personal data can be associated with particular individuals when it is no longer necessary for any business or legal purpose.
- Transfer limitation - Transfer personal data to another country only according to the requirements prescribed under the regulations to ensure that the standard of protection provided to the personal data so transferred will be comparable to the protection under the PDPA, unless exempted.
- Data breach notification - Assess whether a data breach is notifiable and notify the PDPC and/or affected individuals where there is a notifiable data breach.
- Accountability - Make information about the organization's data protection policies, practices and complaints process available on request. Designate one or more individuals as a Data Protection Officer (DPO) to ensure that the organization complies with the PDPA, including the implementation of personal data protection policies within the organization. The business contact information of at least one of such individuals should also be made available to the public.

A data intermediary, which is an organization that processes personal data on behalf of another organization, is generally only required to comply with the protection obligation, the retention limitation obligation, and the data breach

		notification obligation, where it must notify an organization without undue delay of the occurrence of a data breach. The Monetary Authority of Singapore (MAS) also requires licensed insurers and registered insurance brokers to comply with sector-specific requirements, such as: the Notices on Technology Risk Management (FSM-N03 and FSM-N19), which sets out, among others, information on notifying the MAS in the event of a system malfunction or IT security incident involving customer personal information that has a severe and widespread impact on the operations or service to customers; and the Notices on Cyber Hygiene (FSM-N20 and FSM-N04), which set out, among others, security measures such as multi-factor authentication to protect customer information.
	**Taiwan**	Data collectors shall inform the data subject of: (a) the name of the collector; (b) purpose of collection; (c) classification of personal data collected; (d) time period, area, subject and manner of use of such personal data; (e) rights of the data subject and the way to exercise such rights; and (f) influence on the rights of a data subject who decides not to provide personal data. Besides these, data collectors are required to obtain the data subject's informed consent. Obtaining consent is the most common practice to meet the statutory requirement of collecting, processing and using personal data.
	**Thailand**	Under the PDPA, the data controller shall not collect, use or disclose personal data, unless the data subject has given consent prior to or at the time of such collection, use and/or disclosure, except where it is permitted to do so by the provisions of this Act or any other laws. Exceptions to consent for general personal data include the following: 1. It is for the achievement of a purpose relating to the preparation of historical documents or archives for public interest, or for purposes relating to research or statistics, in which the suitable measures to safeguard the data subject's rights and freedoms are put in place and in accordance with the notification as prescribed by the PDP Committee. 2. It is for preventing or suppressing a danger to a person's life, body or health. 3. It is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract. 4. It is necessary for the performance of a task carried out in the public interest by the data controller, or it is necessary for the exercising of official authority vested in the data controller. 5. It is necessary for the legitimate interests of the data controller or any other persons or juristic persons other than the data controller, except where such interests are overridden by the fundamental rights of the data subject to their personal data. 6. It is necessary for compliance with a law to which the data controller is subject. Further, under the PDPA, the collection, use or disclosure of personal data shall not be conducted in a manner that is different from the purpose previously notified to the data subject in accordance with paragraph one, except under the following circumstances: 1. The data subject has been informed of such new purpose, and the consent is obtained prior to the time of collection, use or disclosure.

		2. It can be done by the provisions of this Act or in other laws. The collection of personal data shall be limited to the extent necessary in relation to the lawful purpose of the data controller. Regarding the transfer of personal data, PDPA specifies that if there is a transfer of personal data to other countries, the data controller must comply with a sub-regulation issued by the PDP Committee, and the destination countries or international organization must have adequate personal data protection standards, except in certain circumstances (detailed in question 12).
	**Vietnam**	Obligations vary depending on whether the entity carrying out the collection, use, disclosure and transfer of personal data acts as a data controller (who determines the purposes and means of personal data processing) or a data processor (who processes personal data on the data controller's behalf). More stringent obligations will be imposed on data controllers than on data processors. In short, under the PDPD, data controllers are obliged to comply and demonstrate their compliance with data protection principles such as lawfulness, transparency, purpose limitation, data minimization and anti-sale, accuracy, security, and storage limitation. These principles are elucidated by specific obligations imposed on data controllers, such as obtaining consent or securing another lawful basis for personal data processing (e.g., contract performance), giving prior privacy notice, responding to data subject requests, conducting impact assessment filings and implementing data protection measures, reporting and handling data breaches, and recording and storing system logs of personal data processing. Meanwhile, data processors bear more lightened duties, such as receiving personal data only after an agreement with the controller has been reached, processing personal data in strict accordance with the concluded agreement, applying data protection measures, and deleting or returning all personal data to the controller after finishing the data processing.

6. What are the main requirements for ensuring security of personal data?

China	▪ Keep the personal data collected strictly confidential, and do not disclose, tamper with, damage, sell or unlawfully provide the same to a third party. ▪ Establish and improve a whole-process data security management system, organize data security education and training, and adopt technical and other necessary measures to ensure that data is secure. ▪ Strengthen risk monitoring, and when any data security defect, vulnerability or other risk is discovered, immediately take remedial measures; and when a data security event occurs, immediately take disposition measures, notify users, and report to the appropriate department in a timely manner as required. ▪ Network operators shall fulfil security protection obligations according to the requirements of the multi-levelled protection system for cybersecurity; prevent interference with the network, damage of or unauthorized access to the network; and prevent network data from being divulged, stolen or falsified. ▪ If the entity collecting personal data is an operator of critical information infrastructure (likely to include any insurance company licensed in China), personal data collected or generated in China must be stored and processed within China, and provision of the same to overseas will be subject to security assessment conducted by Chinese regulators. ▪ Encryption measures shall be taken when storing the personal data of children under 14 years old. If the network operator entrusts the processing of children's personal data to a third party, it shall conduct a security assessment.
Hong Kong	Data users must take all practicable steps to ensure that personal data is protected against unauthorized or accidental access, processing, erasure or other use. They include establishing a governance framework on risk identification, assessment and control, continuous monitoring, cybersecurity incident response plan, contingency strategies, and training.
Indonesia	Data users must maintain the secrecy, integrity and availability of personal data that is being managed, which is still a principle-based requirement. There are no further elaborations as to how these requirement thresholds should be performed.
Japan	The APPI states that business operators must take necessary and appropriate measures to prevent leakage, loss or damage of personal data and otherwise ensure proper security management of personal data. This provision is then further built upon in the Guidelines and industry-specific guidelines
Malaysia	Data users shall take practical steps to protect personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction. The data user should also develop and implement a security policy pursuant to the Personal Data Protection Regulations 2013 (Regulations). Data users should, pursuant to the Code, also consider certain factors, including data security management, risk management, access control, physical and electronic security measures, and disaster management plans. Where personal data is processed by a data processor on behalf of a data user, the data user must obtain sufficient guarantees from the data processor in respect of the technical and organizational security measures relating to the processing. The Code recommends that this can be achieved by, among others, imposing contractual obligations on the data processor and/or undertaking regular audits and/or relying on third-party audit reports performed by licensed auditors on the data processor to ensure compliance.

		Insurers are also required to comply with specific requirements imposed by BNM in connection with ensuring the security of customer information. These specific requirements include, among others, the following: ▪ Deploying preventive and detective information and communication technology controls to prevent theft, loss, misuse, unauthorized access, disclosure or modification of customer information, as well as to detect errors and irregularities when they occur ▪ Implementing adequate physical security controls to ensure customer information stored in paper or electronic forms is properly protected against theft, loss, misuse or unauthorized access, modification or disclosure by whatever means ▪ Ensuring that employment contracts contain a provision requiring all employees to sign a confidentiality undertaking that clearly specifies the obligation and requirement of any written law to safeguard customer information as well as the consequences for failure to comply with such obligation and requirement ▪ Performing adequate and relevant due diligence assessment when selecting an outsourced service provider that has access to customer information ▪ Implementing a customer information breach-handling and response plan
	**Philippines**	PICs and personal information processors (PIPs) (any natural or juridical person or any other body to whom a PIC may outsource or instruct the processing of personal data) are required to implement reasonable and appropriate security measures aimed at maintaining the availability, integrity and confidentiality of personal data and intended for the protection of personal data from unlawful destruction, alteration or disclosure, and other unlawful processing. These security measures include: (a) organizational; (b) physical; and (c) technical security measures for the protection of personal data: ▪ Organizational security measures - These include, among others, the appointment of Compliance Officers and/or Data Protection Officers (DPOs) who will be the ones accountable for ensuring compliance with applicable laws and regulations for the protection of data privacy and security, and the putting in place and implementation of in-house data protection policies. The identity of the individual(s) designated as the DPO or DPOs should be made known to any data subject upon request. ▪ Physical security measures - These include, among others, the putting in place of policies and procedures to monitor and limit access to and activities in the room, workstation or facility housing personal data, including guidelines that specify the proper use of and access to electronic media, as well as having the proper design of office space and work stations, which shall provide privacy to anyone processing personal data. ▪ Technical security measures - These shall include, among others, putting in place security policies with respect to the processing of personal data, installing safeguards to protect their computer network against interference or accidental, unlawful or unauthorized usage, regularly monitoring security breaches, and encrypting personal data during storage and while in transit and providing an authentication process. PICs must ensure that PIPs or third-party subcontractors also implement the foregoing measures.
	**Singapore**	Organizations are required to implement reasonable physical, technical and organizational security safeguards to protect personal data and ensure that the level of security is in line with the amount, nature and sensitivity of personal data involved. There is no one-size-fits-all solution, and each organization should consider adopting security arrangements that are reasonable and appropriate in the circumstances by, for example, considering the nature of personal data, the form in

		which the personal data has been collected (e.g., electronic or physical), and the possible impact to the individual concerned if an unauthorized person obtains, modifies or disposes of the personal data. As mentioned in question 5, the MAS also requires licensed insurers and registered insurance brokers to comply with sector-specific requirements, such as the Notices on Cyber Hygiene (FSM-N20 and FSM-N04) which set out, among others, security measures such as multi-factor authentication to protect customer information.
	**Taiwan**	Data collectors shall take appropriate security measures to prevent personal data from being stolen, altered, damaged, destroyed or disclosed, and they shall adopt a personal data protection plan or measures for the handling of personal data and the disposal measures for the personal data after termination of activities related to such personal data.
	**Thailand**	The PDPA specifies that the data controller and data processor must apply security measures to prevent the loss, access, use, change, amendment or disclosure of personal data
	**Vietnam**	Data controllers and data processors must apply relevant technical and management measures to protect personal data, such as developing personal data protection policies, conducting cybersecurity inspection against data processing systems prior to system destruction, appointing a data protection officer and department when sensitive personal data is under processing, reporting and handling data breaches, as well as other applicable protection measures under personal data protection, cyber information security, and cybersecurity regulations (e.g., system classification and monitoring, risk assessment and management).

7. Are there additional requirements with respect to 'sensitive personal data'?

China	The PIPL sets out the following requirements with respect to sensitive personal data: ▪ Personal data processors may not process sensitive personal information unless there are specific purposes, and sufficient necessity and strict protection measures are taken. ▪ An individual's separate consent shall be obtained for processing their sensitive personal data. Where any law or administrative regulation provides that written consent shall be obtained for processing sensitive personal information, such provision shall prevail. ▪ To process sensitive personal data, the data processors must notify individuals of the necessity of the processing of sensitive personal information and the impacts on individuals' rights and interests. ▪ Where a personal data processor processes the personal information of a minor under the age of 14, it shall obtain the consent of the minor's parents or other guardians, as well as develop special personal information processing rules. ▪ To process sensitive personal data, the data processors must conduct personal information protection impact assessment in advance and record the processing information.
Hong Kong	Insurers as data users should implement security safeguards and precautions in relation to the security of customers' personal data held by them and their staff and agents. The security level should reflect the sensitivity of the data and the seriousness of potential harm that may result from a security breach.
Indonesia	Under the PDP Law, the term is called 'specific personal data, ' which consist of health information, biometric data, genetic data, criminal records, child data, personal finance information, and other data deemed specific under a regulation.
Japan	The APPI defines 'special care-required personal information ' (Special Care-Required Personal Information) as personal information comprising a person's race, creed, social status, medical history, criminal record, fact of having suffered damage by a crime, or other descriptions prescribed by the relevant cabinet order as those of which the handling requires special care so as not to cause unfair discrimination, prejudice or other disadvantages to the person. The cabinet order further lists the following information as Special Care-Required Personal Information: mental or physical disabilities; result of medical checks; medical advice, diagnosis or dispensing of pharmaceuticals by doctors based on medical checks; criminal procedures conducted against an individual; and procedures concerning juvenile delinquency against minors. Subject to certain prescribed exceptions, business operators shall not acquire Special Care- Required Personal Information without the data subject's consent. Further, the opt-out arrangement, under which a business operator may transfer personal data to third parties without the data subject's consent if the data subject can opt out from doing so and the business operator complies with certain procedural requirements, is not available for transfer of Special Care-Required Personal Information. The PPC and FSA Guidelines define 'sensitive data ' (Sensitive Data) as Special Care-Required Personal Information, and information on union membership, family status, place of domicile, health and medical care, and sexual orientation (except for the information: (a) disclosed by data subject or national or local government or pursuant to specific provisions of laws; or (b) which is clear from the appearance recognized by sight or photographic means). Insurance companies are not required to collect, use or transfer Sensitive Data unless otherwise provided in the PPC and FSA Guidelines. Further, the opt-out arrangement is not available for the transfer of Sensitive Data.

	**Malaysia**	'Sensitive personal data ' is defined as any information relating to the data subject's physical or mental condition (including thumbprint and DNA profile), political opinions, religious beliefs or other beliefs of a similar nature, and/or the commission or alleged commission by the data subject of any offenses. Processing of sensitive personal data requires the explicit consent of data subjects. The Code recommends that sensitive data be afforded a higher level of security protection.
		
		An insurer is also required by BNM to carry out the following, among others:
		▪ Undertake an independent risk assessment of its end-to-end backup storage and delivery management to ensure that existing controls are adequate in protecting sensitive data at all times.
		▪ Ensure adequate controls and measures are implemented for the storage and transportation of sensitive data in removable media, including the following, among others:
		  ▪ Implementing authorized access control to sensitive data (e.g., password protection, user access matrix)
		  ▪ Deploying the latest industry-tested and accepted encryption techniques

	**Philippines**	The DPA distinguishes between personal information and sensitive personal information, which are treated differently under the law. Sensitive personal information includes personal information about race, ethnic origin, marital status, age, color, religious and political affiliation, health, education, genetic or sexual life, social security numbers, health records, licenses, tax information, and criminal history. Under the DPA, the processing of sensitive personal information generally requires the prior consent of the data subject. Specifically, the processing of sensitive personal information is generally prohibited, except under the following circumstances: ▪ The data subject has given their prior consent. ▪ The processing of sensitive personal information is specifically provided for by existing laws, and the latter do not require the consent of the data subject. ▪ The processing is necessary to protect the life and health of the data subject or another person under limited circumstances. ▪ The processing is necessary to achieve the lawful and non-commercial objectives of public organizations and their associations, provided that the processing is confined to consenting bona fide members only. ▪ The processing is necessary for the purpose of medical treatment. ▪ The processing is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to the government or public authority pursuant to a constitutional or statutory mandate. In addition, where a personal data breach involves sensitive personal data or information that may be used to enable identity fraud that may have been acquired by an unauthorized person or group of people, and such acquisition is likely to give real risk of serious harm to the affected data subjects, the PIC must observe the mandatory reporting and notification requirements under the DPA.
	**Singapore**	'Sensitive personal data' is not defined under the PDPA, and therefore there are no specific requirements for sensitive personal data. However, the PDPC has recognized in its enforcement decisions that certain types of data are more sensitive in nature, such as children's data and financial information. As organizations are required to take appropriate measures bearing in mind the nature and sensitivity of the personal data, such data may thus warrant more stringent security arrangements. For example, in the employment context, it would be reasonable to expect a greater level of security for highly confidential employee

		appraisals as compared to more general information about the projects an employee has worked on. If more stringent requirements are required to be imposed in respect to the processing of these sensitive personal data, such concerns are likely to be addressed in sector-specific laws that apply concurrently. The MAS expects licensed insurers and registered insurance brokers to build strong and effective capabilities to safeguard the integrity and availability of their critical systems and services and protect customer and other sensitive information from unauthorized access. This means having in place measures to protect their critical systems, detect threats and system vulnerabilities in a timely manner, and recover from cyber-attacks swiftly. Regular security reviews and tests must also be conducted to ascertain the continued effectiveness of these measures.
	**Taiwan**	Unless otherwise permitted by law, personal data in connection with the data subject's medical history, medical treatment, genetic information, sexual life, physical examination and criminal record cannot be collected, processed or used. Under the Insurance Act, with the data subject's written consent, the collection, processing and use of the data subject's personal data in connection with their medical history, medical treatment and physical examination (unless such consent exceeds the necessary scope of the specific purpose; the collection, processing or use merely with the consent of the data subject is prohibited by other statutes; or such consent is against the data subject's will) are permitted if it falls under any of the following categories: 1. Insurance companies, insurance agents, brokers and surveyors that operate or practice business per the Insurance Act 2. The juristic persons commissioned by insurance companies to provide assistance in confirming or performing their obligations under an insurance contract 3. Insurance-related entities established with the permission of the FSC to handle disputes and matters relating to compensation for victims of motor vehicle accidents
	**Thailand**	Collection of personal data pertaining to race; ethnic origin; political opinions; cult, religious or philosophical beliefs; sexual behavior; criminal records; health data; disability; trade union information; genetic data; biometric data; or any data that may affect the data subject in the same manner as prescribed by the PDP Committee is prohibited without the explicit consent of the data subject, except under the following circumstances: 1. It is to prevent or suppress a danger to the life, body or health of the person, where the data subject is incapable of giving consent for whatever reason. 2. It is carried out in the course of legitimate activities with appropriate safeguards by the foundations, associations or any other not-for-profit bodies with political, religious, philosophical or trade union purposes for their members, former members of the bodies, or persons having regular contact with such foundations, associations or not-for-profit bodies in connection with their purposes, without disclosing the personal data outside of such foundations, associations or not-for-profit bodies. 3. It is information that is disclosed to the public with the explicit consent of the data subject. 4. It is necessary for the establishment, compliance, exercise or defense of legal claims.

5. It is necessary for compliance with a law to achieve the purposes with respect to the following:

   a. Preventive medicine or occupational medicine, the assessment of the employee's working capacity, medical diagnosis, the provision of health or social care, medical treatment, the management of health or social care systems and services

      In the event that it is not for compliance with the law, and such personal data is under the responsibility of the occupational or profession practitioner or person having the duty to keep such personal data as confidential under the law, it must be for compliance with the contract between the data subject and the medical practitioner.

   b. Public interest in public health, such as protecting against cross-border transmission of dangerous diseases or epidemics that may be contagious or pestilent, or ensuring standards or quality of medicines, medicinal products or medical devices, on the basis that there is a provision of suitable and specific measures to safeguard the rights and freedom of the data subject, and in particular maintaining the confidentiality of personal data in accordance with the duties or professional ethics

   c. Employment protection, social security, national health security, social health welfare of the entitled person by law, the road accident victim's protection, or social protection in which the collection of personal data is necessary for exercising the rights or carrying out the obligations of the data controller or the data subject, by providing suitable measures to protect the fundamental rights and interest of the data subject

   d. Scientific, historical or statistic research purposes, or other public interests that must be carried out only to the extent necessary to achieve such purposes, and where suitable measures have been provided to protect the fundamental rights and interests of the data subject as prescribed by the PDP Committee

   e. Substantial public interest, by providing suitable measures to protect the fundamental rights and interest of the data subject

Additionally, the PDPA specifies that if the data controller collects personal data relating to criminal records, they must comply with a sub-regulation issued by the PDP Committee, which sets out specific definition of 'personal data relating to criminal records' and relevant requirements for collecting such data (e.g., consent, retention period).

Vietnam

A personal data protection officer and department must be appointed when sensitive personal data is under processing. Their contact details must also be notified to the competent authority.

Under the PDPD, 'sensitive personal data' refers to personal data associated with an individuals' privacy that, when infringed upon, will directly affect the legitimate rights and interests of that individual, including the following:

- Political and religious opinions
- Information concerning health status and private life included in the medical records, excluding information on blood type
- Information concerning racial and ethnic origin
- Information concerning inherited or acquired genetic characteristics of an individual

- Information concerning the physical traits and biological characteristics of an individual
- Information concerning the sex life and sexual orientation of an individual
- Data about crimes and criminal acts collected and stored by law enforcement agencies
- Customer information of credit institutions, foreign bank branches, payment intermediary service providers or other authorized organizations, including: customer identification information as prescribed by laws, information on accounts, information on deposits, information on deposited assets, information on transactions, information on organizations and individuals that are guarantors at credit institutions, bank branches, or payment intermediary service providers
- Location data of an individual as determined by location services
- Other personal data as specified by laws to be specific and required necessary security measures

8. Are there additional obligations imposed on insurance companies with respect to collection, use and transfer of personal data of customers? Are there any registration requirements to be complied with?

China	The main requirements set out in question 5 are applicable to insurance companies. According to Measures for the Regulation of the Internet Insurance Business, insurance companies shall comply with the following obligations: ▪ Indicate the information with respect to the measures for the protection of consumers' personal information, insurance application trading information and trading security in a conspicuous position on its self-operated network platform for internet insurance business. ▪ Ensure that the service access place of its self-operated network platform is located within the territory of the People's Republic of China. ▪ Submit a report on the operations of its internet insurance business of the previous year to the information system relating to internet insurance regulation before 30 April each year, including information regarding cybersecurity construction and information system operation and failure. Moreover, there are specific requirements for life insurance companies and intermediaries to ensure the authenticity of the personal data of life insurance policyholders, and for life insurance companies to manage and use customer information in a legitimate, reasonable, safe and confidential manner. Finally, under the Administrative Measures for Health Insurance, an insurance company may neither illegally collect or obtain genetic information and genetic testing data of the insured except for the family's genetic history, nor require the applicant, the insured or the beneficiary to provide the above information for the purpose of selling health insurance products.
Hong Kong	The main requirements set out in question 3 are applicable to insurance companies. If customers are required to supply their personal data to an insurer, they should be provided with a personal information collection statement stating clearly certain prescribed information (e.g., purpose of the data collection). Insurers should also formulate and make available their privacy policy statements stating in detail information such as the main purposes of use of each type of personal data held
Indonesia	The main requirements set out in question 5 are applicable to insurance companies. In addition, insurance companies having cooperation with third parties in the use of information technology will need to ensure that such third parties maintain the security of all information, including the confidentiality of the insurance company and consumer's personal data.
Japan	The main requirements set out in question 5 are applicable to insurance companies. The PPC and FSA Guidelines recommend that consent to use personal information beyond the scope of the purpose of use or transfer of the personal data to third parties be obtained in writing.
Malaysia	The main requirements set out in our response to question 5 are applicable to insurance companies. If customers are required to supply their personal data to an insurer, they should be issued with a written notification containing the Prescribed Matters in relation to the processing of their personal data by the insurer. In addition, insurers must also be registered with the Regulator pursuant to the PDPA.

		Some of the additional requirements imposed by BNM in connection with ensuring the security of customer information are set out in our response to question 6.
	**Philippines**	The requirements as discussed above are applicable to insurance companies, as they fall under the definition of PICs. Moreover, an entity (a PIC or a PIP) that operates in the Philippines is required to register with the NPC its DPO and its data processing systems if it meets any of the following criteria: ▪ It has at least 250 employees. ▪ It processes the sensitive personal information of at least 1,000 data subjects. ▪ It is processing personal data on a regular basis. ▪ It is processing personal data that is likely to pose a risk to the rights and freedoms of the data subjects. As regards the transfer of personal data of customers, the rules on data sharing or data outsourcing/subcontracting, as the case may be, should be complied with. This includes, but is not limited to, the execution of the appropriate data transfer agreements. With respect to the collection of personal information from consumers by insurance providers as a result of electronic commerce activities, IC Circular Letter No. 2014-47 of 2014 (Guidelines on Electronic Commerce of Insurance Products) expressly provides that the DPA shall govern the same. Electronic commerce refers to any commercial activity that involves buying, selling or providing insurance products and services online or via the internet. Furthermore, insurance companies and agents are required under the Insurance Code and the 2013 Market Conduct Guidelines to ensure protection over their clients' personal information. They are also prohibited from discussing, disclosing or otherwise utilizing such information with any other person outside of the company. The privacy policy statement must be made clear to their customers/clients and made easily accessible to them. Under the Bill of Rights of Policyholders, policyholders are protected from unauthorized disclosure of personal, financial and other confidential information by insurance companies, intermediaries and soliciting agents, except as otherwise allowed by law, regulations, or valid court or government order.
	**Singapore**	The main requirements set out in question 5 are applicable to insurance companies. Note that the Life Insurance Association of Singapore has also released Codes of Practice and a Code of Conduct for life insurers and tied agents of life insurers in respect of the PDPA.
	**Taiwan**	The requirements stipulated above apply to insurance companies. Further, besides obtaining the data subject's consent to prove that they have performed their obligations to inform the data subject about the required information, insurance companies may use the following methods to prove the performance of the obligation to inform: (a) phone conversation recording; (b) distribution of insurance policy along with data protection notice; or (c) incorporating the insurance policy and data protection notice into one document to be signed by the data subject. With respect to non-sensitive personal data, consent does not have to be in writing; however, it is suggested to obtain written consent for evidentiary purpose. Note that the Life Insurance Association and the Non-Life Insurance Association of Taiwan have also released the respective template of Notifications for Performance of the Obligations under the PDPL for life insurers and non-life insurers to ensure compliance with their notification obligations and satisfy the consent requirements. There are no particular registration requirements to be complied with.
	**Thailand**	The data controller shall not collect, use or disclose personal data without the data subject's consent prior to or at the time of such collection, use and/or disclosure, except where it is permitted to do so by the provisions of this Act or any other laws (detailed in question 5 and 7).

Apart from the consent requirement (or exceptions to consent as the case may be), in order to legally collect personal data, the data controller is also required to comply with other key obligations under the PDPA, which include the following:

1. Notifying the data subject of the required details before or at the time of such collection, except where the data subject already knows of such details (e.g., the purpose of the collection, use or disclosure of the personal data; the personal data to be collected and the data retention period; the categories of persons or entities to whom the collected personal data may be disclosed; the rights of the data subject)
2. Implementing appropriate security measures (detailed in question 6)
3. Maintaining Records of Processing Activities (RoPAs)
4. Notifying the PDP Committee in case of any personal data breach (detailed in question 21)
5. Having in place a data processing agreement with a data processor (where applicable) (detailed in question 17)
6. Appointing a qualified Data Protection Officer (DPO) (where applicable) (detailed in question 9)
7. Where the data controller is not in Thailand, appointing a representative who is in Thailand and is authorized to act on behalf of the data controller who is outside Thailand

Vietnam

Aside from the general obligations regarding the collection, use and transfer of personal data (as discussed above), the Law on Insurance Business provides certain requirements applicable to insurance companies licensed in Vietnam, as follows:

- For the purpose of building up a database of the insurance industry, the collection, use, storage and provision of information included in the database must ensure confidentiality and security of information and comply with the regulatory provisions of laws on protection of individual privacy, personal secrets, family secrets and trade secrets. State agencies, other organizations and individuals are required to use the information provided for the right purposes and are not allowed to provide information to any third party without the consent of the policyholder or the insured, unless otherwise provided by the law.
- Insurance companies are obliged to protect and keep confidential information provided by the policyholders and/or the insureds, unless requested [to provide] by state agencies or when obtaining consent of the policyholder or the insured.

9. Are insurance companies required to have a data protection officer?

China	A personal data processor processing the personal information reaching the following threshold shall appoint a person in charge of personal information protection: ▪ If the data processor's primary business involves the processing of personal information and whose size of the workforce is greater than 200 employees ▪ If the data processor processes personal information of more than 1 million people, or is expected to process personal information of more than 1 million people within a 12-month period ▪ If the data processor processes sensitive personal information of more than 100,000 people If an insurance company processes data with respect to genes, biometrics and diseases, which may fall under 'important data,' it is required to specify a person in charge of data security and a data security management body. In addition, insurance companies are required to appoint a chief information officer or a person who is mainly responsible for IT-related work. According to the Cybersecurity Law and the Provisions on the Cyber Protection of Personal Information of Children, insurance companies will also need to designate certain personnel to take charge of cybersecurity management and protection of children's personal data (if insurance companies collect personal information of children under 14). Insurance companies are also advised to consider appointing a person in charge of personal information protection according to the best practice proposed under the Information Security Technology - Personal Information Security Specification (GB/T 35273-2020).
Hong Kong	Yes. Where personal data is or is to be collected from a customer, practicable steps should be taken to ensure that the customer is explicitly informed of the name and contact details of the data protection officer who shall be responsible for handling data access or data correction requests made by the customer.
Indonesia	Theoretically, yes, since insurance companies process specific personal data (i.e., personal financial information). As a general rule under the PDP Law, data controllers and data processors must appoint a data protection officer if: (i) they process personal data for public service interest; (ii) their main activity has a nature, scope and/or purpose that requires regular and systematic monitoring over large-scale personal data; and (iii) their main activity includes large-scale processing of specific personal data and/or personal data related to a crime. In addition, insurance companies are also required to have a compliance director who will be accountable to the OJK to ensure that insurance companies are compliant with all prevailing laws and regulations in Indonesia, including the data privacy regulations.
Japan	Under the PPC and FSA Guidelines, insurance companies are required to have: (a) a data protection officer who is in charge of the security management of personal data; and (b) persons who are in charge of managing personal data in the departments handling personal data. Under the PPC and FSA Guidelines, insurance companies are recommended to have a department or committee that oversees the examination and improvement of handling of personal data.
Malaysia	Yes. As part of the application for registration with the Regulator as discussed in our response to question 8, there is a requirement for companies to designate a compliance person within the organization. In addition, the senior management of an insurer is to designate a person of sufficient ranking with overall responsibility for, among others, the implementation

		and ongoing maintenance of policies, procedures and controls with regard to safeguarding customer information (i.e., chief data officer or chief information officer). An insurer must also designate a Chief Information Security Officer (or its equivalent) to be responsible for the technology risk management function of the insurer.
	**Philippines**	Insurance companies, as PICs, must designate a DPO — the individual accountable for the organization's compliance with the DPA. The appointment of a common DPO for a group of related companies is allowed, provided that a compliance officer for privacy who will be supervised by the DPO is also appointed for each member of the group. The identity of the individual(s) so designated should be made known to any data subject upon request.
	**Singapore**	Yes. All organizations, including insurance companies, are required to designate at least one DPO to be responsible for ensuring that the organization complies with the PDPA. This DPO may be a person whose scope of work solely relates to data protection, or a person in the organization who takes on this role as one of their multiple responsibilities.
	**Taiwan**	The PDPL does not impose this requirement on insurance companies. However, it is recommended that an insurance company appoint a specific person in charge of handling such matters.
	**Thailand**	Insurance companies must appoint a data protection officer as their core activity is the collection, use or disclosure of personal sensitive data.
	**Vietnam**	Yes. It is required if the insurance companies process sensitive personal data.

10. Do insurance companies need to undertake privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of personal data?

China	Where an insurance company is involved in any of the following activities, undertaking privacy impact assessments is required: ▪ Processing sensitive personal data ▪ Using personal data to conduct automated decision-making ▪ Commissioning personal data processing, providing personal data to other personal information processors, or disclosing personal data ▪ Providing personal data to an overseas recipient In addition, insurance companies are advised to undertake privacy impact assessments under the following circumstances according to the best practice proposed under the Information Security Technology - Personal Information Security Specification (GB/T 35273-2020): ▪ Prior to the release of products and services, or significant changes in business functions ▪ When there is a significant change in the business model, information system or operating environment ▪ When a significant personal information security incident occurs
Hong Kong	Privacy impact assessments are not expressly required under the PDPO but have become a widespread privacy compliance tool that insurers are advised to adopt before launching any new systems or technologies.
Indonesia	Theoretically, yes, as insurance companies collect and process specific personal data (e.g., personal financial information). As a general rule under the PDP Law, data controllers must conduct a data privacy impact assessment if their processing activities, which include the following, have a potentially high risk toward data subjects: (i) automatic decision-making process that creates a legal effect or a significant effect toward data subjects; (ii) processing of specific personal data; (iii) large-scale personal data processing; (iv) personal data processing for evaluation, scoring or systematic monitoring over a data subject; (v) personal data processing for matching or combining a group of data; (vi) use of new technology in personal data processing; and/or (vii) personal data processing that limits the implementation of rights of the data subjects. In addition, the OJK requires financial services companies to conduct a risk management implementation in the use of information technology that is customized based on the purpose, business policy, size and complexity of the company's business.
Japan	Privacy impact assessments are not expressly required.
Malaysia	Privacy impact assessments are not expressly required under the PDPA. However, this is recommended to ensure that personal data is processed in compliance with the PDPA. Under the RMIT policy document, BNM requires insurers to (among others) carry out the following: ▪ Establish a methodology for rigorous system testing prior to deployment to ensure the system meets user requirements and performs robustly (e.g., application security testing, integration testing)

		▪ Where new information systems and/or technologies are implemented in connection with the offering of internet insurance services for the first time, submit prescribed notifications to BNM
	**Philippines**	Yes. NPC Circular No. 2023-06 provides that a privacy impact assessment should be undertaken for every processing system of a PIC or PIP that involves personal data. The assessment need not be submitted to the NPC, but it shall be made available by the PIC upon the NPC's request arising from investigations or compliance checks.
	**Singapore**	Yes, from a PDPA perspective, privacy impact assessments are required in two scenarios: a. When relying on deemed consent by notification b. When relying on the legitimate interests exception to collect, use and disclose personal data without consent For reference to what a DPIA for (a) could look like, see Annex-B--Assessment-Checklist-for-Deemed-Consent-by-Notification-1-Feb-2021.pdf (pdpc.gov.sg). For reference to what a DPIA for (b) could look like, see Annex-C--Assessment-Checklist-for-Legitimate-Interests-Exception-1-Feb-2021.pdf (pdpc.gov.sg). There could also be other practical situations where insurance providers may consider conducting a DPIA – see the PDPC's Guide to Data Protection Impact Assessments which can be accessed here: Guide-to-Data-Protection-Impact-Assessments-14-Sep-2021.pdf (pdpc.gov.sg). Note that the MAS assesses financial institutions' cyber resilience through both on-site and off-site supervision. Where any gaps or areas of improvement are identified, the MAS requires the financial institution to develop a remedial plan of action and will monitor the financial institution's progress in its implementation. The MAS also monitors the prevailing cyber threat landscape and issues targeted advisories to financial institutions. For instance, the MAS has issued Circular No. SRD TR 01/2015 on Early Detection of Cyber Intrusions and Circular No. SRD TR 03/2015 on Technology Risk and Cyber Security Training for Board to the Chief Executive Officers of all financial institutions.
	**Taiwan**	While insurance companies provide e-commerce services, security measures shall be adopted to protect personal data, including procedures for verification and confirmation of application of technology systems. Moreover, insurance companies are required to take security measures to ensure that personal data is protected under the PDPL. Thus, it is advisable to conduct privacy impact assessments.
	**Thailand**	Privacy impact assessments are not required under the PDPA. Data controllers must review their security measures as needed or when the technology has changed.
	**Vietnam**	Yes. It is needed if the implementation of new information systems and/or technologies for the processing of personal data results in a change to the content of the previously submitted impact assessment(s).

11. What are data subjects' rights, if any, in relation to the processing of their personal data?

China	Data subjects have the following rights: ▪ Right to know and the right to decide on the processing of their personal data ▪ Right to restrict or refuse the processing of their personal data by others ▪ Right to consult and duplicate their personal data from personal data processors ▪ Right to request personal data processors to correct or supplement their personal data when a data subject finds that their personal data is incorrect or incomplete Right to request personal data processors to delete their personal data when a data subject finds that their personal data has been collected or used in breach of applicable laws and regulations or the agreement with the data collector, or the processing purpose has been achieved, or the retention period of their personal data has expired.
Hong Kong	Data subjects have the following rights: ▪ Right to be notified of the purpose and classes of persons to whom the data may be transferred ▪ Right to access their personal data ▪ Right to make corrections to personal data. Data subjects also have the right to opt out from direct marketing.
Indonesia	Data subjects have the following rights: ▪ Right to access their personal data ▪ Right to correct their personal data ▪ Right to deem personal data be treated as confidential information ▪ Right to access historical information on personal data that has been collected ▪ Right to withdraw, revoke or amend consents previously given ▪ Right to reject processing with automatic decision making ▪ Right to be forgotten ▪ Right to file claims with the data user if the data user fails to perform its obligation (e.g., maintain the secrecy of the data)
Japan	Personal data processed by business operators must be disclosed to the data subjects upon their request in writing or by other means acceptable to the data subjects. If retained personal data is found to be incorrect, such personal data must be corrected while remaining in compliance with the purpose of use. If a purpose of use is found to have been violated, the business operator may have to discontinue using its retained personal data to the extent necessary to redress the violation. If a data subject requests disclosure of their information or modifications to their information, the business operator must, in principle, comply with such requests, except under the following circumstances: ▪ The disclosure is likely to harm the life, body, property or other rights or interests of the data subject or a third party. ▪ The disclosure is likely to seriously impede the proper execution of the business of the business operator. ▪ The disclosure violates other laws and regulations.

Malaysia	In general, and subject to certain prescribed exceptions, data subjects have the following rights: ▪ Right of access to personal data - Data subjects are entitled to be informed by the insurer whether their personal data is being processed by or on behalf of the insurer. ▪ Right to correct personal data - Data subjects are entitled to correct their personal data if it is inaccurate, incomplete, misleading or not up to date. ▪ Right to withdraw consent - Data subjects are entitled to withdraw their consent to the processing of personal data. ▪ Right to prevent processing likely to cause damage/distress - Data subjects are entitled to request the insurer to cease the processing of their personal data should the same cause or likely cause substantial damage to them or another, and the said damage/distress is unwarranted. ▪ Right to prevent processing for purposes of direct marketing - Data subjects are entitled to request that the insurer cease or not begin processing their personal data for direct marketing purposes.
Philippines	Under the DPA, data subjects have the following rights: ▪ Right to be informed - right to be informed whether personal data pertaining to a data subject shall be, are being, or have been processed, including the existence of automated decision-making and profiling ▪ Right to access - right to reasonable access to, upon demand of a data subject, personal data that is being processed and other relevant information thereon (such as the sources thereof, names and addresses of the recipients, reasons for disclosure) ▪ Right to correction or rectification - right to dispute the inaccuracy or error in the personal data and have the PIC correct it immediately and accordingly (unless the request is vexatious or otherwise unreasonable) ▪ Right to object - right of a data subject to object to the processing of their personal data, including the right to be notified and given an opportunity to withhold consent to the processing in case of changes or any amendment to the information supplied or declared to the data subject ▪ Right to erasure and blocking - right of a data subject to suspend, withdraw or order the blocking, removal or destruction of their personal data from the PIC's filing system ▪ Right to damages - right to be indemnified for any damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data, taking into account any violation of their rights and freedoms as data subjects ▪ Right to data portability - right to obtain from the PIC a copy of their personal data and/or have the same transmitted from one PIC to another, in an electronic or structured format that is commonly used and allows further use by the data subject
Singapore	In general, data subjects have the right to decide which organizations can collect their data, how it is to be used, and whether it can be disclosed. Under the PDPA, data subjects' rights include the following: ▪ Right to withhold consent from an organization to collect, use or disclose their personal data ▪ Right to be notified by organizations on the purposes for which their personal data will be collected, used and disclosed

		▪ If prior consent has been given, the right to withdraw consent for the organization to continue collecting, using or disclosing such personal data, with reasonable notice ▪ Right to request access to personal data in the possession or under the control of the organization, and information about the ways in which that personal data has been or may have been used or disclosed by the organization within a year before the date of the individual's request ▪ Right to request correction of an error or omission in personal data held by the organization ▪ In addition, it should be noted that under the Purpose Obligation (see our response to question 5 above), organizations may collect, use or disclose personal data about a data subject only for purposes that: ▪ A reasonable person would consider appropriate in the circumstances ▪ Where applicable, that the data subject has been informed of by the organization In addition, there is also a Data Portability Obligation, which allows individuals to transmit the individual's data that is in the organization's possession or under its control, to another organization in a commonly used machine-readable format. This Data Portability Obligation will only take effect when corresponding regulations are issued.
	**Taiwan**	According to Article 3 of the PDPL, the following rights should be exercised by the data subject with regard to their personal information and should not be waived in advance or limited by a specific agreement: ▪ Inquiry and request for a review of the personal information ▪ Request to make duplications of the personal information ▪ Request to supplement or correct the personal information ▪ Request to discontinue collection, processing or use of personal information ▪ Request to delete the personal information
	**Thailand**	Under PDPA, data subjects have certain rights, such as the following: ▪ Right to withdraw their consent at any time ▪ Right to access or obtain copy of the personal data concerning them from the data controller, or to request the disclosure of the acquisition of the personal data obtained without their consent ▪ Right to data portability, that is, to send or transfer data to a third party ▪ Right to object to the collection, use or disclosure of their personal data at any time in cases where the personal data is collected: (1) with exemption; (2) for the purpose of direct marketing; or (3) for purposes relating to study and research in respect of sciences, history or statistics ▪ Right to erase, destroy or anonymize personal data to de-identify the data subject ▪ Right to restrict the use of the personal data ▪ Right to request the data controller to ensure that the personal data remain accurate, up to date, compete and not misleading ▪ Right to file a complaint with the competent authority.
	**Vietnam**	Under PDPD, a data subject, unless otherwise provided by laws, has the following rights: ▪ Right to know about the processing of its data

- Right to give consent
- Right to access to view, edit or request the edits of its personal data
- Right to withdraw consent
- Right to delete data or request to delete its personal data
- Right to restrict processing of its personal data
- Right to be provided with data by requesting the data controller and data processor to provide its personal data
- Right to object to data processing to prevent or restrict the disclosure of its personal data or the use of its personal data for marketing or advertising purposes
- Right to complain, denounce, initiate a lawsuit; to claim for damages; to self-protection.

Data transfer and outsourcing

12. Are there any restrictions regarding cross-border transfers of personal data for insurance companies?

China	If the entity collecting personal data is an operator of critical information infrastructure (likely to include any insurance company licensed in China), personal data collected or generated in China must be stored and processed within China, and provision of the same overseas will be subject to a security assessment by Chinese regulators.
Hong Kong	The transfer of data outside of Hong Kong is restricted under the PDPO, though this restriction is not yet effective.
Indonesia	Offshore data transfers may only be conducted if any of the following requirements is met: (i) the nation where the receiving party is located has a similar or the same standard of personal data protection as the PDP Law; (ii) there is sufficient and binding data protection provisions; or (iii) there is consent from the data subject. In theory, insurance companies must coordinate with the MOCI to do cross-border data transfer. The coordination includes reporting the plan and result of the cross-border data transfer. In practice, this coordination exercise has not been fully implemented. Further, insurance companies must keep its data centers located in Indonesia, unless approved otherwise by the OJK.
Japan	The APPI provides that personal data may not be transferred to a foreign country unless: (a) the data subject has given specific advance informed consent to the transfer of the data subject's personal data to the entity in a foreign country; (b) the country in which the recipient is located has a legal system that is deemed equivalent to the Japanese personal data protection system, designated by the PPC; or (c) the recipient undertakes adequate precautionary measures for the protection of personal data, as specified by the PPC. In relation to (b), under the Guidelines, EU countries and the UK have been designated as countries that have a legal system deemed equivalent to the Japanese personal data protection system.
Malaysia	Generally, the data subject's consent must be obtained for transfer of personal data outside of Malaysia, unless the transfer is to a 'whitelist' country prescribed by the Minister. Though no such list has been officially issued thus far, a public consultation paper that includes a draft initial 'whitelist' of jurisdictions has been issued. Further, as described in our response to question 16, the Outsourcing policy document and Guidelines on Data Management and MIS Framework issued by BNM will have to be complied with if the personal data is being stored or processed by a third party/outsourcing party.
Philippines	The DPA does not appear to specifically require that personal information collected from Philippine citizens or residents be stored or processed in the Philippines. It also does not appear that the DPA prohibits the offshore storage or the transfer of such personal information to foreign jurisdictions. The DPA, however, considers the PIC to continue to be responsible for personal information that may have been 'transferred to a third party for processing, whether domestically or internationally.' The general rules on data sharing (between PICs) and data outsourcing/subcontracting (from PIC to a PIP) will apply. For data sharing, affected data subjects must be notified of the details of processing before data is transferred or at the next practical opportunity; and the sharing must be supported by an appropriate legal basis for processing personal and/or sensitive personal

		information. The NPC also highly recommends the execution of a data sharing agreement (see Item 13). For data outsourcing or subcontracting, the agreement between the PIC and PIP must comply with the mandatory formalities prescribed by Section 44 of the DPA IRR. There is an old law, Presidential Decree No. 1718 (PD 1718), which prohibits the transfer of 'any and all documents and information possessed by or in the custody of Philippine corporations, entities or individuals doing business in the pursuit of the national economic development programs of the government and/or engaged in the development, promotion, protection and export of Philippine products to increase foreign currency revenues' to any foreign person or government, except if the taking, sending or removal: (a) is consistent with and forms part of a regular practice of furnishing to a head office or parent company or organization outside of the Philippines; (b) is in connection with a proposed business transaction requiring the furnishing of the document or information; (c) is required or necessary for negotiations or conclusion of business transactions, or is in compliance with an international agreement to which the Philippines is a party; or (d) is made pursuant to the authority granted by the designated representative(s) of the president of the Philippines. The Office of the President has yet to issue rules and regulations implementing PD 1718 since its passage on 21 August 1980. Hence, the law is not strictly enforced.
	Singapore	Note that no personal data should be transferred out of Singapore, unless the Transfer Limitation Obligation (see question 5) is observed.
	Taiwan	Processing and use of personal data internationally by insurance companies are subject to the PDPL. In general, after performing the obligation to inform and obtaining the data subject's consent (written consent is recommended for evidentiary purposes), insurance companies are allowed to transfer personal data across borders. However, the competent authorities may prohibit cross-border transfers of personal data under the following circumstances: (a) where substantial national interests are involved; (b) where the international treaties or agreements specify otherwise; (c) where the rights and interests of the data subject are likely to be damaged as a result of the data recipient country not having appropriate laws and regulations to protect personal data; or (d) where the PDPL may be avoided because the personal data is transmitted or used by way of indirect transmission to a third country or area.
	Thailand	The PDPA specifies that if personal data is transferred to other countries, the data controller must comply with a sub-regulation issued by the PDP Committee, and the destination countries or international organization must have adequate personal data protection standards, except under the following circumstances: 1. It is for compliance with a law. 2. The consent of the data subject has been obtained, provided that the data subject has been informed of the inadequate personal data protection standards of the destination country or international organization. 3. It is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract. 4. It is for compliance with a contract between the data controller and another person or juristic person for the interests of the data subject. 5. It is to prevent or suppress a danger to the life, body or health of the data subject or other persons, when the data subject is incapable of giving the consent at such time.

		6. It is necessary for carrying out the activities in relation to substantial public interest. In addition, if the data controller and data processor have set a policy for sending or transferring personal data to the affiliate in other countries for a joint business operation, and if such policy has been examined and certified by the PDP Committee, the sending and transferring are exempted from complying with adequate personal data protection standards as explained above.
	**Vietnam**	If personal data constitutes state secrets, an approval from competent authority can be required for cross-border transfer of data. Otherwise, there are no specific restrictions regarding the cross-border transfer of personal data. The PDPD imposes an overseas data transfer filing requirement applicable to the cross-border transfer of a Vietnamese citizen's personal data on the data transferor; there is, however, no prior approval required for such transfer. That said, the authority can take action to suspend the transfer if the filing obligation is not appropriately discharged.

13. Are there any specific requirements for insurance companies in relation to the use and transfer of personal data for marketing purposes? Can customers opt-out?

China	When business operators form 'user profile' for marketing, the characterization of the subject of personal data in the user profile should not contain obscenity, pornography, gambling, superstition, terrorism, violence or expression of discrimination against ethnicity, race, religion, disability or disease. Business operators that provide goods/services to PRC consumers (including insurance companies) should only send marketing messages to the recipients with their consent. Data subjects have the right to request business operators to stop sending marketing messages, and business operators must comply upon receipt of such request. If automated decision-making and relevant algorithmic technologies are involved in the marketing, the business operators shall conduct privacy impact assessments in advance, ensure the data subjects' right to refuse, and shall not launch 'big data ripening' or discriminatory pricing.
Hong Kong	A data user (e.g., an insurer) must not use or provide personal data to another person for use in direct marketing unless it has obtained the data subject's consent. If an insurer intends to use the personal data of its customers in direct marketing, it must inform the customers of its intention to use the data. Certain prescribed information must be provided to the customers. A response channel (e.g., an opt in / opt out box or a telephone hotline) must be provided so that the customers may, without charge, communicate whether they consent to the intended use.
Indonesia	Specific consent from the data owner to use and transfer personal data for marketing purposes is required, and it must be an opt-in consent.
Japan	Other than general provisions dealing with transferring personal information to third parties, there are no specific provisions dealing with direct marketing. Please note, however, that sending of advertisement emails is regulated by a separate law called the Act on Regulation of Transmission of Specified Electronic Mail. Under this act, advertisement emails may not be sent unless prior consent of the recipient is obtained.
Malaysia	An insurer (i.e., a data user) must not use or transfer personal data for direct marketing purposes unless it has obtained the data subjects' consent. All marketing communications sent to data subjects must contain an 'unsubscribe'/'opt-out' option, which allows data subjects to choose not to receive such communications or subsequent marketing messages. Further, data subjects may, at any time, by a notice in writing to the data user, request to cease processing their personal data for purposes of direct marketing.
Philippines	Generally, with respect to the use of personal information for direct marketing, all data subjects are required under the DPA to be provided specific information regarding the purpose and extent of processing of their personal data, including, where applicable, the processing of their personal data for purposes of direct marketing. Moreover, when data is shared by a PIC to third parties for purposes of direct marketing (or any other commercial purpose), the NPC highly recommends that there be an express 'data-sharing agreement' between the PIC and the third party to whom such data is shared. NPC Circular No. 2020-03 prescribes formal requirements in the execution of the data sharing agreement. The data sharing agreement should be executed by the PICs and witnessed by their respective Data Protection Officers. Moreover, the data sharing agreement should contain the following provisions: ▪ Purpose and lawful basis of the data sharing

		▪ Objectives of the data sharing ▪ Parties to the DSA ▪ Term or duration of the DSA ▪ Operational details of the data sharing, including the procedure the parties intend to observe in implementing the same ▪ Description of the reasonable and appropriate organizational, physical and technical security measures that the parties intend to adopt to ensure the protection of the shared data ▪ Mechanisms that allow affected data subjects to exercise their rights relative to their personal data ▪ Rules for the retention of shared data and for the secure return, destruction or disposal of the shared data and the timeline therefor. Use and transfer of personal data for marketing purposes must be supported by an appropriate legal basis for processing personal and/or sensitive personal information. If the basis for processing is consent and the consent is withdrawn, a PIC must immediately cease processing. The rights of the data subject to withdraw consent and to object to the processing, in this case, is absolute. In addition, IC Circular Letter No. 2014-47 provides for the following rules regarding the use of client/customer information for marketing purposes: ▪ Section 11.1. Insurance companies are prohibited from sending marketing emails to consumers without their consent, except when insurance providers have an existing relationship with them. ▪ Section 11.2. Any marketing email messages sent shall prominently display a return email address and shall provide in plain language a simple procedure by which consumers can notify insurance providers that they do not wish to receive such messages.
	**Singapore**	An organization should obtain express opt-in consent for the use and disclosure of personal data for marketing purposes. Customers may opt out from receiving marketing material. The organization may not, as a condition of providing a product or service, require individuals to consent to the collection, use or disclosure of their personal data beyond what is reasonable to provide that product or service. An organization must comply with the 'Do Not Call' requirements when sending any marketing messages by way of phone call, fax or text message to a Singapore telephone number. The sending of unsolicited commercial communications in bulk (beyond the prescribed threshold) by email, text or multimedia messaging to mobile telephone numbers is subject to the Spam Control Act. Note that no personal data should be transferred out of Singapore, unless the Transfer Limitation Obligation (see question 5) is observed.
	**Taiwan**	Joint promotion – Disclosure, transfer or exchange of clients' personal data shall require prior consent (written consent is recommended for evidentiary purposes). Co-selling – Where an insurance company co-sells with its associated companies, the collection, processing and use of customers' personal data are subject to the PDPL. Direct response marketing – Upon conducting direct response marketing, the PDPL will apply. Direct response marketing representatives shall inform the data subject of the relevant information as required by PDPL and obtain their consent. TV marketing –The PDPL applies to the sale of insurance products on TV. Yes, the customer can opt-out. When the customer expresses rejection, the insurance companies must cease using such customer's personal data for marketing purposes.

	**Thailand**	The data subject shall have the right to object to the collection, use or disclosure of personal data at any time if the collection, use or disclosure is for direct marketing purposes. In addition, if consent is the lawful basis the data controller relies on for the collection, use or disclosure of their personal data for direct marketing, the data subject shall have the right to withdraw consent at any time.
	**Vietnam**	Aside from the general obligations regarding the collection, use and transfer of personal data, more stringent requirements will be imposed on: (i) advertising services (regarding the scope of data allowed to be used as well as the details of privacy disclosures that must be communicated to the data subjects); and (ii) direct advertising via messages (SMS, MMS, USSD), calls and emails (regarding the checking of the 'Do-Not-Call Register' list, registration of a name identifier, as well as embedment of mandatory information and function into an advertising message/email/call).

14. Are there any specific requirements for insurance companies in relation to the receipt of personal data from their business partners?

China	When data processors (including insurance companies) receive personal data from their business partners, they should verify to ensure that the personal data provided by the third party is from legitimate sources, such as whether the third party has obtained the consent of the data subject to obtain the data and the data shared has not exceeded the scope of the data subject's consent to processing. The data processors (including insurance companies) shall also clearly delineate responsibilities for data security with the third party and adopt strict access control measures and rights management.
Hong Kong	If an insurer is planning to use the data received from a business partner for direct marketing, the insurer must be notified in writing by the business partner that: (a) the business partner has given written notice to data subjects and obtained their written consent to the provision of personal data; and (b) the use of the personal data is consistent with the consent obtained from the data subject.
Indonesia	Insurance companies should seek appropriate assurance from its business partners that the data subjects have consented to the provision of such personal data to insurance companies and to the processing, or the use, of the personal data by insurance companies.
Japan	Subject to certain prescribed exceptions, business operators must, when they receive personal data from third parties, confirm the following matters: (a) the name or appellation and address of the third party, and for a corporate body the name of its representative; and (b) circumstances under which the personal data was acquired by the third party. The Guidelines further recommend that business operators assess legal compliance by third parties, such as purpose of use, disclosure procedure and disclosure of inquiry or complaint counter. Business operators must also keep a record of the date when it received the personal data, a matter concerning the confirmation, and other matters prescribed by the rules of the PPC.
Malaysia	The Code recognizes that where an insurer receives personal data from certain prescribed categories of business partners, consent is deemed to have been given by the data subject to disclose the personal data to the insurer and for the insurer to process the same. That said, an insurer planning to use the data received from a business partner should still seek appropriate assurances from its business partners that the data subjects have consented to the provision of such personal data to the insurer and the processing of the personal data by the insurer.
Philippines	If an insurance company obtains personal data from its business partners, the parties must enter into either a data sharing agreement (if the insurance company would independently act as a personal information controller) or an outsourcing/subcontracting agreement (if it will act as a processor on behalf of its business partners), as the case may be. Note that the execution of a data sharing agreement is not required. Nevertheless, the NPC said that it incentivizes PICs who execute a data sharing agreement, as it is a best practice and a demonstration of accountability among the parties to the data sharing. Moreover, the NPC takes into account whether such an agreement was executed in case a complaint is filed pertaining to such data sharing and/or in the course of any investigation relating thereto, as well as in the conduct of compliance checks. In any event, the company should ensure that the transfer of personal data complies with the provisions of the DPA, including the business partners' obtaining the specific consent of the data subject for such transfer, unless another legal basis for processing personal and/or sensitive personal information is present.

Singapore	The organization should ensure that it complies with key obligations of the PDPA in respect of any personal data that it has collected from its business partners. In particular, the organization should satisfy itself that the business partner has obtained the relevant consent of the individuals to the disclosure of the personal data to the insurer in respect of the processing by the organization for the specified purpose
Taiwan	While insurance companies receive personal data from third parties other than data subjects (e.g., business partners), insurance companies shall inform the data subject of: (a) the source of the personal data; (b) the name of the collector (i.e., the insurance companies); (c) the purpose of collecting the data; (d) the classification of the personal data collected; (e) the time period, area, subject and manner of use of such personal data; and (f) the rights of the data subject as well as how such rights are exercised and the data subject's consent is obtained. For compliance purposes, the insurance companies must also ensure that their business partners have obtained sufficient consent from data subjects to transfer personal data to the insurance companies.
Thailand	There are no specific requirements. However, under PDPA, the data controller shall not collect, use or disclose personal data without the data subject's consent prior to or at the time of such collection, use and/or disclosure, except where it is permitted to do so by the provisions of this Act or any other laws (detailed in question 5).
Vietnam	There are no specific requirements. However, insurance companies must ensure that their business partners have notified and obtained sufficient consent from data subjects to transfer personal data, unless another legal basis applies (e.g., contract performance). If the transferring business partners act as the data processors of the insurance companies, a data processing agreement must also be reached between the parties.

15. Can insurance companies transfer the personal data of their insurance agents or intermediaries to other service providers, such as investigation agents or debt collectors?

China	Yes, provided that the following requirements are met: ▪ The transfer is consistent with the notification given to data subjects and the consent obtained. ▪ The transfer is compliant with the restrictions on cross-border personal data transfer. ▪ The responsibilities and obligations of data recipients are set out, for example, through contracts.
Hong Kong	Insurers should ensure that the transfer of data to and the use of such data by investigation agents or debt collectors are consistent with the personal data collection statements that were given to such agents or intermediaries at the time personal data was collected, and that such investigation agents or debt collectors must not use the data beyond such purpose.
Indonesia	Yes, provided that insurance companies have obtained specific consents from the data owners regarding such transfer of personal data to their insurance agents or intermediaries.
Japan	Subject to the respective requirements under the relevant regulations and guidelines, insurance companies can: (a) collect the personal data from their insurance agents or intermediaries; and (b) transfer such personal data to service providers (please see question 14 for data collection and question 5 for data transfer). If the personal data is transferred to credit agencies, insurance companies need to obtain the data subjects' consent. Insurance companies must represent on the consent letter that the data will be transferred to the member companies of the credit agencies and the names of the member companies that will use the personal data. Insurance companies may not use the opt-out arrangement for transfer of information on an individual's repayment ability to credit agencies.
Malaysia	Yes, subject to the insurer having obtained the consent of the insurance agents or intermediaries. Please also refer to the response to question 6 relating to personal data processed by data processors.
Philippines	There is no specific provision/restriction regarding this transfer. Generally, insurance companies, as PICs, are bound to comply with the conditions under the DPA with regard to the processing of personal information and sensitive personal information of data subjects. Specifically, the sharing or transfer of personal data to a third party by a PIC requires the existence of an appropriate legal basis for processing personal and/or sensitive personal information (as the case may be). Furthermore, the service providers to whom such personal data are transferred will likely be deemed as PIPs and will likewise have to comply with the conditions under the DPA concerning the processing of personal data. The data outsourcing or subcontracting agreement between insurance companies and the service providers must comply with the requirements under Section 44 of the DPA IRR.
Singapore	Yes. However, notification to and/or valid consent from the data subject may be required. For any transfer of personal data overseas, please see the response to question 12.

	**Taiwan**	The PDPL applies only to personal data of natural persons. When transferring the personal data of insurance agents or intermediaries who are natural persons to other service providers, insurance companies need to notify such persons of the relevant information as required by the PDPL and mentioned above. Please also refer to the responses to questions 5 and 12.
	**Thailand**	Under the PDPA, the data controller can collect, use or disclose personal data if the data subject has given consent prior to or at the time of such collection, use and/or disclosure, except where it is permitted to do so without consent by the provisions of the PDPA or any other laws (detailed in question 5). In addition, if the data controller that instructs other service providers who act as its data processor, the data controller must arrange for an agreement between them (detailed in question 17).
	**Vietnam**	Yes, if the data subject has consented or as requested by the authorities, or if another legal basis applies (e.g., contract performance).

16. Are there additional requirements imposed with respect to the outsourcing of data processing to third-party data processors?

China	Such transfer shall be: (a) consistent with the notification given to data subjects and the consent obtained; and (b) compliant with the restrictions on cross-border personal data transfer. Where insurance companies outsource data processing to third-party data processors, they shall ensure that the following requirements are met: ▪ The responsibilities and obligations of third-party data processors are set out, for example, through outsourcing contracts. ▪ Such third-party data processors meet the company's internal control requirements formulated in compliance with various regulatory requirements and shall assume responsibility for internal control risks arising out of such outsourcing business. The insurance companies oversee the personal data processing activities of the third-party data processors. Insurance companies that outsource IT services shall formulate sound management systems for the outsourcing of IT services to mitigate any risks that may arise and adopt a reasonable and prudent approach to outsourcing IT services. Moreover, insurance companies shall, in accordance with requirements of CBIRC and based on their actual need for outsourcing services, develop basic rules for outsourcing services to secure their control over the information system. Where an insurance company outsources any content in its information system that involves sensitive information, such as state secrets, its trade secrets or customer privacy, it shall comply with relevant laws, regulations and requirements of the state and competent regulatory authorities, and such outsourcing shall be subject to approval by the decision-making body of the company. If the outsourcing of IT services involves 'material outsourcing' such as outsourcing of data center and information technology infrastructure, the insurance company shall formally report to CBIRC when preparing for implementation of material outsourcing (i.e., before the implementation of such material outsourcing).
Hong Kong	Data users must adopt contractual or other means to prevent any personal data transferred to a data processor from being kept longer than is necessary, and also to prevent unauthorized or accidental access, processing, erasure and loss, among others. Insurers should also ensure that such outsourcing complies with the Guideline on Outsourcing (GL14) issued by the Insurance Authority
Indonesia	Specific consents from the data owners regarding such transfer of personal data to the third-party data processors are required. Insurance companies must also comply with the applicable outsourcing requirements issued by the OJK. In addition, any outsourcing activities by insurance companies must be included in their business plan and approved by the OJK.
Japan	Where a business operator entrusts the handling of personal data under its control, in whole or in part, to another party, such party is considered a 'subcontractor' for the purpose of the APPI. For the transfer of personal data to a subcontractor, data subjects' consent is not required. However, the business operator must exercise necessary and appropriate supervision over the subcontractor to ensure proper security management of the personal data.
Malaysia	Please refer to the response to question 6 relating to personal data processed by data processors. Insurers are also required to comply with the relevant policy documents issued by BNM, including the Outsourcing policy document, the Guidelines on Data

		Management and MIS Framework, and the policy document on Management of Customer Information and Permitted Disclosures.
	**Philippines**	PICs may subcontract or outsource the processing of personal data to a third-party data processor or PIP, provided that the PIC uses contractual or other reasonable means to: ensure that proper safeguards are in place; ensure the confidentiality, integrity and availability of the personal data processed; prevent its use for unauthorized purposes; and generally comply with the requirements of the DPA, the DPA IRR, other applicable laws for processing of personal data, and other issuances of the NPC. The DPA also requires that the relationship between the PIC and PIP be covered by an express outsourcing agreement, that is, a contract or other legal act that binds the PIP to the PIC. Section 44 of the DPA IRR sets forth the requirements to be considered in such outsourcing agreements. The PIC remains responsible for the personal data outsourced to third parties. Further, under IC Circular Letter No. 2019-54, insurance companies are required to submit to the IC reports on their existing outsourcing agreements as of 31 December of every calendar year on or before 31 March of the next succeeding calendar year.
	**Singapore**	Yes. The outsourcing of data processing will likely constitute outsourcing by the insurance company, which is subject to the MAS Guidelines on Outsourcing. These guidelines on outsourcing set out MAS' expectations on a financial institution that has entered into outsourcing or is planning to outsource its business activities to a business provider. The disclosing organization remains responsible for the personal data outsourced to third parties and must ensure that there are appropriate contractual controls in relation to the use and protection of the personal data disclosed. Under the PDPA, an organization has the same obligations under the PDPA in respect of personal data processed on its behalf by a third-party data intermediary as if the personal data were processed by the organization itself. As such, it is good practice for an organization to undertake an appropriate level of due diligence and to impose the relevant contractual obligations to assure itself that a potential third-party data processor is capable of complying with the provisions of the PDPA.
	**Taiwan**	Yes. Such transfer shall be: (a) consistent with the notification given to data subjects and the consent obtained; and (b) compliant with the restrictions on cross-border personal data transfer under the PDPL. Moreover, outsourcing the processing of customers' data to a third-party data processor will constitute outsourcing by the insurance company, which is subject to the requirements under the FSC's Guidelines Governing Operations Outsourcing by Insurance Enterprises. Prior approval from the FSC will generally be required if the outsourcing arrangements involve/relate to the following: (a) natural person customers' data; (b) material IT systems; and (c) the offshore location of such outsourcing.
	**Thailand**	Yes. Notifications from the Office of Insurance Commission (OIC) mention this issue. The outsourcing of data processing is permitted but the insurers must follow certain requirements, including having their criteria for selecting service providers, concluding an agreement in writing, requiring the service provider to follow the insurers' security measures, gradually auditing and monitoring the service provider, and notifying the OIC at least 30 days in advance. Prior approval from the OIC is required and other detailed requirements must be complied with if the services provided are for conducting online sales (or electronically supporting online sales), issuing policies, lending money or paying compensation electronically. In addition, under the PDPA, the data processor shall have the following duties: 1. To proceed with the collection, use or disclosure of personal data under an instruction received from the data controller

		2. To arrange for appropriate security measures to prevent loss, access, use, modification, amendment, or the illegitimate or unauthorized disclosure of personal data, and to notify the data controller of the violation of personal data so arisen 3. To arrange for and keep a record of personal data processing activities according to the bases and procedures prescribed by the PDP Committee. Please refer to question 17 for the data controller's obligation to enter into a data processing agreement with its data processor in case of the outsourcing of the third-party data processor.
	**Vietnam**	Other than the general obligations regarding the collection, use and transfer of personal data (as discussed above), there must be a data processing agreement concluded with the outsourced data processors. The data processors must also be declared in the data controller's impact assessment submitted to the authority, as accompanied by the corresponding data processing agreements.

17. Do insurance companies have to ensure third parties meet certain standards in outsourcing processing to third parties? Are there additional safeguards to be taken?

China	Yes. Insurance companies shall conduct a security assessment before engaging an external outsourcing service provider. Where insurance companies outsource data processing to third-party data processors, they shall ensure that such third-party data processors meet the company's internal control requirements formulated in compliance with various regulatory requirements and shall assume responsibility for internal control risks arising out of such outsourcing business. In addition, insurance companies shall oversee the personal data processing activities of the third-party data processors. Insurance companies are required to enter into outsourcing contracts with the service provider, specifying the scope of outsourcing services, security and confidentiality requirements, protection of intellectual property, business continuity, dispute resolution and transitional arrangement when the contract is terminated or amended. Insurance companies are not allowed to assign IT security management responsibilities to the outsourcing service provider.
Hong Kong	An insurer is required to exercise due diligence and care in selecting the relevant service provider, and should take into account factors such as reputation, experience, financial soundness, managerial skills, and technical and operational expertise in the process of selecting the service provider. The insurer should also ensure that it and the service provider have proper safeguards in place to protect the integrity and confidentiality of the insurer's information and customer data.

Indonesia	Insurance companies are required to exercise due diligence and care in selecting the relevant service provider before that provider is appointed, such that an appointed provider has sufficient capability and expertise to provide the service in a manner that also complies with the prevailing laws and regulations, including the data privacy regulations. The outsourcing of personal data processing to third parties does not release insurance companies from the obligation to maintain the secrecy, integrity and availability of personal data being managed, which is a principle-based requirement.
	
	In addition, the service provider shall comply with the following requirements:
	▪ Has qualified experts supported by certification of expertise academically or professionally
	▪ Willing to provide access to the following so that they can obtain the required data and information in a timely manner:
	  ▪ Insurance company's internal auditor
	  ▪ External auditor
	  ▪ Insurance company's group internal auditor
	  ▪ The OJK.
	▪ Expresses no objection if the OJK and/or other parties, who are in accordance with the provisions of laws and regulations are authorized to carry out inspections, will carry out inspections
	▪ Maintains the security of all information, including the confidentiality of the insurance company and the consumer's personal data

Japan	Under the PPC and FSA Guidelines, insurance companies are required to establish certain standards in selecting the outsourcees. Insurance companies are also required to periodically monitor whether the outsourcees comply with the standards and supervise them.

Malaysia	Yes — please refer to our response to question 16.
Philippines	Yes. Under the DPA, PICs are responsible and accountable for personal information under their control or custody, even when it has been transferred to a third party or PIP for processing, subject to cross-border arrangement and cooperation. As such, PICs must ensure that third parties offer a comparable level of protection while the information is being processed by the latter. Furthermore, IC Circular Letter No. 2014-47 provides that when insurers transfer personal information to third parties, they shall remain responsible for the protection of that information so transferred. Insurers must ensure, through contractual or other means, that the third parties comply with the privacy provisions under insurance regulations and the applicable laws on data privacy.
Singapore	Yes. Note that the MAS' Outsourcing Guidelines may apply to insurers regulated by MAS. Please refer to our response to question 16. Organizations should ensure that third parties are bound by appropriate contractual obligations to guarantee compliance with the PDPA.
Taiwan	Yes. In outsourcing operations to third parties, insurance companies must ensure that the third parties comply with the provisions of the PDPL and applicable laws and regulations, adopt an internal control and internal audit system as required by law, and establish mechanisms for the protection of clients' rights and for handling client disputes. When selecting the relevant service provider, the insurance companies should exercise due diligence and consider factors such as reputation, experience, financial soundness, managerial skills, technical and operational expertise, and whether the service provider has relevant certificates for information security or privacy management. Moreover, the insurance companies are required to enter into outsourcing contracts with the service provider, specifying the scope of outsourcing services, security and confidentiality requirements, protection of intellectual property, audit rights, customer dispute resolution, and transitional arrangement when the contract is terminated or amended.
Thailand	In assigning third parties as data processors in carrying out works, insurance companies as the data controllers must arrange for an agreement between them so that the works are carried out in line with the PDPA (detailed in question 16). Insurance companies are also required to issue a protocol to be followed by the outsourcer.
Vietnam	The general obligations on the collection, use and transfer of personal data would apply (as discussed above). In addition, the Law on Insurance Business requests the insurance companies to be solely responsible for, among others, protecting and keeping confidential customers' data in connection with its outsourced activities.

Data retention

18. What is the data retention requirement?

China	PIPL provides that the personal data retention period should be the minimum period required to fulfil the relevant purpose, and when such period expires, the personal data should be deleted. Data retention by insurance companies shall also comply with relevant regulatory requirements. For instance, financial institutions shall preserve customers' identities materials and transaction records for the following periods: ▪ Customers' identities materials shall be preserved for at least five years from the year in which a business relationship closes or a one-off transaction is entered into an account. ▪ Transaction records shall be preserved for at least five years from the year in which a transaction is entered into an account. Where its customers' identities or any of its transaction records are involved in a suspicious transaction activity that is under anti-money laundering investigation, and such investigation has not been completed when the minimum preservation period expires, the financial institution shall preserve the information until the anti-money laundering investigation work is completed. In addition, the Insurance Law of the PRC generally requires that the term to keep the books, original certificates and relevant information concerning business activities shall be no less than five years for businesses with an insurance period of one year or less, and no less than 10 years for businesses with an insurance period of more than one year, starting from the date of termination of the insurance contract.
Hong Kong	A data user must take all practicable steps to erase personal data no longer required for the purpose for which the data was used, unless the erasure is prohibited under any law or public interest requires otherwise.
Indonesia	The requirement is five years for data retention. In addition, Regulation 20 requires stored customer data to be encrypted; currently, however, the minimum encryption requirement has yet to be established.
Japan	Under the APPI, business operators must maintain certain records of transfers or receipt of personal data to or from third parties for a period prescribed by the relevant PPC rules from the date they created the record. Under the insurance regulations, insurance companies are required to maintain certain reports and business forms for the statutory retention period. Under the PPC and FSA Guidelines, insurance companies are recommended to designate the retention period of personal data depending on the purpose of use of such personal data.
Malaysia	Personal data processed for any purpose shall not be kept longer than is necessary for the fulfillment of that purpose. Thus, the insurer should take steps to destroy or permanently delete personal data if it is no longer required, unless such retention is necessary for its operational, audit, legal, regulatory, tax or accounting requirements. If personal data is retained but not utilized to fulfil the purposes for which it was collected, or after a period where there is no longer a need for the personal data to be kept, fresh consent of data subjects must be obtained.
Philippines	Generally, under the DPA, personal data shall be retained only for as long as necessary: (a) for the fulfillment of the purposes for which it was obtained, or when the processing relevant to such purpose has been terminated; (b) for the establishment, exercise or defense of legal claims; or (c) for legitimate business

		purposes that must be consistent with standards followed by the applicable industry or approved by the appropriate government agency. While personal data may be retained for a certain period pursuant to legitimate business purposes, such purpose must be consistent with standards followed by the applicable industry. Taking into consideration the technical challenges, companies must start considering strategies on how to make data erasure possible, or how to put in place measures to prevent further processing of data on archival media/backup tapes. The DPA provides that personal data shall not be retained longer than necessary. Where data is being retained, PICs should document its justification and ensure that data subjects are fully notified of such retention, of the purpose, and of other relevant information
	**Singapore**	An organization should cease to retain its 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 the purpose for which that personal data was collected is no longer being served by the retention of the personal data, and retention is no longer necessary for legal or business purposes.
	**Taiwan**	Unless otherwise provided by law, when the purpose of collecting personal data no longer exists or the term for the specific purpose expires, insurance companies shall delete or cease the processing and use of the personal data. However, insurance companies may not delete or cease using personal data if they need the personal data to perform their business operations or if written consent is obtained from the data subject. Upon the expiration of the data retention period, if there is a need to continue processing and using personal data due to handling of complaints, mediation, litigation and other procedures, the retention period may be extended to the date of completion of such dispute-handling or a specific date as stipulated under the relevant laws.
	**Thailand**	The data controller must inform the data subject about the period for which the personal data will be retained, prior to or at the time of such collection. If it is not possible to specify the retention period, the expected data retention period according to the data retention standard shall be specified.
	**Vietnam**	In general, the data custodian must delete stored information upon the request of the data subject and/or once the purpose of the data's use has been accomplished and/or the specified storage period expires and/or in other circumstances prescribed by laws necessitating data deletion; it must also notify the data subject of such deletion. General archiving regulations will apply. In addition, Vietnam has a data localization requirement. Under the Cybersecurity Law and its guiding Decree No. 53/2022/ND-CP, domestic and foreign enterprises providing certain types of cyberspace services must localize certain types of user data in Vietnam if statutory triggering conditions are met. For domestic enterprises, these conditions include the fact that they: (a) provide services on the telecom network, the internet and value-added services on cyberspace in Vietnam; and (b) collect, exploit, analyze or process (i) personal information, (ii) data about users' relationships or (iii) data generated by users in Vietnam. When it comes to foreign enterprises, more requirements must be met before the data localization obligation can be triggered, including but not limited to the failure to cooperate with a competent authority to handle a cybersecurity violation.

19. Are there regulatory requirements to have local data centers and disaster recovery processes?

China	Insurance companies established and licensed within China are required to establish data centers and disaster recovery centers within the territory of China. Insurance companies are also required to establish and implement detailed internal rules and systems concerning security management of data centers and disaster recovery centers, safety management of IT assets and network security management, including preparing disaster recovery plans, establishing data backup system, testing on the disaster recovery technical scheme, etc.
Hong Kong	There are currently no regulatory requirements to have local data centers. The transfer of data outside of Hong Kong is restricted under the PDPO, though this restriction is not yet effective. Insurance companies conducting insurance activities over the internet should ensure that there are appropriate backup procedures for the database to guarantee that proper book records can be maintained. Under GL20, insurance companies should develop a cybersecurity incident response plan, which covers scenarios of cybersecurity incidents and corresponding contingency strategies to maintain and restore critical functions and essential activities in such scenarios. The plan should also include criteria for the escalation of the response and recovery activities to the board of directors or its designated management team.
Indonesia	Insurance companies are required to store personal data within data centers and disaster recovery centers situated in Indonesia, unless approved otherwise by the OJK. Insurance companies can use third-party data center service providers.
Japan	There are currently no regulatory requirements to have local data centers. Under the PPC and FSA Guidelines, insurance companies are required to have certain recovery measures.
Malaysia	The PDPA does not legally prescribe such requirements. However, in implementing practical security measures in relation to the processing of personal data, the Code recommends as a guiding principle the establishment of a disaster management plan, which includes implementing measures and procedures for the containment and recovery of personal data for damage limitation purposes. However, BNM has issued policy documents setting out the requirements on disaster recovery processes and the reporting requirements that the insurer must comply with in connection with specified technology-related breaches or incidents.
Philippines	The DPA does not specifically require the establishment of local data centers in the Philippines. With respect to disaster recovery processes, NPC Circular No. 16-03 on Personal Data Breach Management requires all PICs and PIPs to establish and implement a 'Security Incident Management Policy,' which collectively refers to all the policies and procedures implemented by a PIC or PIP to govern the actions to be taken in case of a security incident or personal data breach. Specifically, a PIC or PIP shall implement policies and procedures for the purpose of managing security incidents, including personal data breaches. These policies and procedures must ensure the following: ▪ Creation of a data breach response team, with members that have clearly defined responsibilities, to ensure timely action in the event of a security incident or personal data breach ▪ Implementation of organizational, physical and technical security measures and personal data privacy policies intended to prevent or minimize the occurrence of a personal data breach and assure the timely discovery of a security incident

		▪ Implementation of an incident response procedure intended to contain a security incident or personal data breach and restore integrity to the information and communications system ▪ Mitigation of possible harm and negative consequences to a data subject in the event of a personal data breach ▪ Compliance with the DPA, the DPA IRR, and all related issuances by the NPC pertaining to personal data breach notification Further, NPC Circular No. 2023-04 requires the creation of a Business Continuity Plan to mitigate potential disruptive events. It must consider, among others, disaster recovery, privacy, business impact assessment, and crisis communications plan.
	**Singapore**	The MAS Notice 127 on Technology Risk Management (FSM-N03) mentioned in question 5 requires an insurer to put in place a framework and process to identify critical systems, and to meet certain standards in respect of the availability of the critical systems, such as ensuring that the maximum unscheduled downtime for each critical system that affects the insurer's operations or service to its customers does not exceed a total of four hours within any period of 12 months, and to establish a recovery time objective of not more than four hours for each critical system. Having effective disaster recovery processes is also part of the overall assessment the MAS would have regard to in respect of the risk management framework of the financial institution, and whether it has adequate business continuity plans in place. The Technology Risk Management Guidelines may also be relevant for consideration as the MAS sets out its minimum expectations and guidance for managing technology and cyber risks in these guidelines.
	**Taiwan**	Upon satisfying legal requirements and obtaining the FSC's special approval in accordance with the Guidelines Governing Operations Outsourcing by Insurance Enterprises, insurance companies can establish data centers outside of Taiwan. When the FSC approves the insurance companies' outsourcing arrangements and if the data involves any Taiwanese natural person customers' data, the insurance companies are generally required to have a backup of such data in Taiwan, unless they obtain the FSC's special approval for exemption. If personal data is stolen, altered, damaged, destroyed or disclosed, insurance companies shall adopt precautionary and remedial measures that shall be reviewed and examined by an independent professional. Insurance companies should also establish disaster recovery processes and appropriate backup procedures as part of their risk management controls to maintain and restore critical functions and essential activities and continue to provide services to customers.
	**Thailand**	There are no requirements to have local data centers and disaster recovery processes under the PDPA. Insurance companies, however, are required by the OIC's Notification on IT Risk Management to have a disaster recovery plan and to ensure that the companies have sufficient data for the continuity of service provision in case of emergency.
	**Vietnam**	There is no specific requirement to establish local data centers in Vietnam. However, Vietnam has a data localization requirement that generally requires certain enterprises to store data within the territory of Vietnam for a specified period (see question 18 above). Regarding disaster recovery processes, the Cybersecurity Law requires that service providers in cyberspace formulate/develop plans and solutions to promptly resolve cybersecurity incidents.

Data breach management

20. What are the consequences of a data privacy breach? Is it a criminal offense? What is the penalty?

China	Under the PIPL, violations of personal data protection provisions may lead to confiscation of illegal gain and a fine of up to RMB 1 million (along with fines of up to RMB 100,000 for responsible individuals), and in serious cases, suspension of business or revocation of business license and fines of up to RMB 50 million or 5% of turnover of the previous year (along with fines of up to RMB 200,000 for responsible individuals). Under the DSL, violations of data security protection obligations may lead to a fine of up to RMB 500,000 (along with fines of up to RMB 100,000 for directly responsible individuals), and in serious cases, suspension of business or revocation of business license and fines of up to RMB 2 million (along with fines of up to RMB 200,000 for directly responsible individuals). Where the national core data management system is violated, compromising national sovereignty, security and development interests, a fine of up to RMB 10 million and suspension of business or revocation of business license may be imposed. Unauthorized cross-border transfer of data may result in confiscation of illegal gain and a fine of up to RMB 1 million (along with fines of up to RMB 100,000 for direct responsible individuals), and in serious cases, suspension of business or revocation of business license and fines of up to RMB 10 million (along with fines of up to RMB 1 million for directly responsible individuals). Serious breach of personal data protection requirements could lead to criminal liabilities for both the entity and the responsible person(s) (up to seven years' fixed-term imprisonment).
Hong Kong	The PCPD may serve an enforcement notice to direct the data user to remedy the contravention of DPPs. Contravention of an enforcement notice is an offense. Certain other specific breaches under the PDPO also constitute criminal offenses. Contravention of an enforcement notice could result in a fine of HKD 50,000 and imprisonment for two years.
Indonesia	A data privacy breach is not a criminal or civil offense if it is not due to a violation by the company. The criminal offense is with the party that tries to access the personal data without authorization. Further, insurance companies are required to notify data subjects of any data breach under the PDP Law. The notification must be done within 72 hours. Specifically for insurance companies, violations (or failures to comply) are subject to administrative sanctions imposed by the OJK. These include warning letters; restriction of business activities (in part or in whole); blacklisting of certain individuals or parties from being shareholders, directors, commissioners or senior management of insurance companies; or revocation of business licenses.
Japan	The APPI requires certain breaches of personal data to be notified to the competent authority and affected individuals. A data breach does not constitute a criminal offense of a company that experienced the breach in general, while the attacker who caused the breach can be subject to sentences of imprisonment (with labor) of not more than one year, or a fine for not more than JPY 500,000 under the APPI, or criminal penalties under other laws prohibiting unauthorized access to computer systems.
Malaysia	A data privacy breach constitutes a breach of the Security Principle, which is an offense, and on conviction attracts a fine not exceeding MYR 300,000 and/or imprisonment for a term not exceeding 2 years.

	**Philippines**	In case of unauthorized access or intentional breach, imprisonment ranging from one year to three years and a fine of not less than PHP 500,000 but not more than PHP 2 million shall be imposed on persons who knowingly and unlawfully, or violating data confidentiality and security data systems, break in any way into any system where personal and sensitive personal information are stored. Some personal data breaches must be reported to the NPC and notified to the affected data subjects. A penalty of imprisonment ranging from one year and six months to five years, and a fine of not less than PHP 500,000 but not more than PHP 1 million shall be imposed on persons who, after having knowledge of a security breach and of the obligation to notify the NPC, intentionally or by omission conceal the fact of such security breach.
	**Singapore**	A data privacy breach could affect the MAS' view of the risk management within the insurance company and may result in the MAS taking various regulatory actions in response to the breach. A breach of the protection obligation is not a criminal offense. If the PDPC finds that an organization is in breach of any of the data protection provisions in the PDPA, it may give the organization such directions as it thinks appropriate to ensure compliance. These directions may include requiring the organization to carry out the following: ▪ Stop collecting, using or disclosing personal data in contravention of the PDPA ▪ Destroy personal data collected in contravention of the PDPA ▪ Provide access to or correct the personal data ▪ Pay a financial penalty of an amount not exceeding SGD 1 million, or 10% of the organization's local annual turnover if this exceeds SGD 10 million Where the PDPC has reasonable grounds for suspecting that an organization is in breach of the PDPA, it may also require the organization to produce specified documents or to provide specified information by written notice. The PDPC also has powers enabling it to enter premises and to gain access to information, documents and equipment or articles relevant to an investigation. Do note that following are criminal offences under the PDPA: ▪ Contravention of the Do Not Call provision - A fine not exceeding SGD 10,000 and/or imprisonment for a term not exceeding three years may be imposed. ▪ Submitting an access or correction request to obtain access or change the personal data about another individual without the authority of the individual - A fine not exceeding SGD 5,000 and/or imprisonment for a term not exceeding 12 months may be imposed. ▪ Alteration, falsification, concealment, disposal of or destruction of records containing personal data or about the collection, use or disclosure of personal data with an intent to evade an access or correction request - A fine not exceeding SGD 5,000 for individuals and SGD 50,000 for organizations may be imposed. ▪ Obstruction or making false or misleading statements - A fine not exceeding SGD 10,000 for individuals and SGD 100,000 for organizations may be imposed. Individuals may also be imprisoned for a term not exceeding 12 months. ▪ Knowing or reckless unauthorized disclosure of personal data; knowing or reckless unauthorized use of personal data for a wrongful gain or wrongful loss to any person; and knowing or reckless unauthorized re-identification of anonymized data - A fine not exceeding SGD 5,000 and/or imprisonment for a term not exceeding two years may be imposed.

Taiwan	A breach of the key obligations of the PDPL, which may harm other people's rights, is a criminal offense. Depending on what offense under the PDPL a violator committed and the severity of the situation, the criminal penalty that a violator might be subject to includes a sentence of imprisonment and a monetary fine. For example, PDPL violations may result in a fine of up to NTD 1 million (approximately USD 33,333) and/or imprisonment of up to five years. Additionally, if the FSC finds that an insurance company is in breach of the data protection provisions in the PDPL, it may impose administrative penalties as it thinks appropriate on such insurance company, which includes: (a) ordering corrections to be made within a specified timeframe; and (b) a monetary fine up to NTD 15 million (approximately USD 462,400). Civil liability (e.g., damages and class actions) may apply if the data subject sues the violator for any breach of the PDPL.
Thailand	If the data controller or the data processer fails to comply with the PDPA, it could face civil liabilities with punitive damages, administrative fines of up to THB 5 million (approximately USD 156,790), and criminal penalties that include imprisonment of up to one year or a fine of up to THB 1 million (approximately USD 31,358), or both.
Vietnam	Criminal penalties will likely not apply unless the infringement constitutes: (i) interception or unauthorized access of a person's communications (mail, telephone, telegraphic); (ii) unlawful uploading or use of information on computer networks and telecommunications networks; or (iii) unlawful collection, possession, exchange, trade, or publication of information about bank accounts. Penalties can be in the form of monetary fine of up to VND 1 billion (approximately USD 41,000) or seven years of imprisonment, or prohibition against holding certain positions for up to five years. Administrative penalties vary depending on the actual data privacy infringements, including but not limited to monetary fines that can rise to VND 100 million (approximately USD 4,000). Notably, the draft decree on administrative sanctions against cybersecurity violations ('Draft CASD') can subject a data privacy offender to a fine of 5% of the total revenue of the preceding fiscal year in Vietnam. Additional sanctions and remedial measures under the Draft CASD include, among others, license revocation, confiscation of means used to process personal data, suspension of business from one to 24 months, and mandatory cessation of data processing for one to three months. Civil sanctions (e.g., compensation) may apply if the data subject sues the data custodian

21. Is there a statutory obligation to disclose data breaches to regulators?

China	Under the DSL, if a data security event occurs, data processors shall report the same to the competent authority. Under the CSL, if personal information has been or may be divulged, damaged or lost, network operators shall report the same to the competent authority. If the data breach constitutes a cybersecurity incident, the network operator shall also report to the competent authority. For data processors processing data with respect to genes, biometrics and diseases, which may fall into 'important data,' regular risk assessments with respect to data processing activities shall be conducted, and risk assessment reports shall be submitted to the competent authority. Under the Provisions on the Cyber Protection of Personal Information of Children, insurance companies shall inform the competent authority where there were or are likely to be breaches of children's personal data that caused or may cause any serious consequence. Moreover, if any employee of a life insurance company or insurance broker accesses or uses customer data beyond the permitted scope or discloses or resells customer information, and such conduct may have constituted a crime, the life insurance company or insurance broker shall hand the employee over to the judicial authority.
Hong Kong	There is no statutory obligation to disclose data breaches to the PCPD. However, under GL20, upon the detection of a cybersecurity incident, insurance companies should report the incident, together with the related information, to the Insurance Authority as soon as practicable, and in any event no later than 72 hours from detection. According to GL20, 'cybersecurity incident' refers to an event that threatens the security of the system of an insurance company, which includes leakage of data in electronic form, denial of service attack, compromise to protected information systems or data assets, malicious destruction or modification of data, abuse of information systems, massive malware infection, website defacement, and malicious scripts affecting networked systems.
Indonesia	Yes. Under the PDP Law, a data breach must be notified to the Data Protection Authority. However, at the time of publication of this guide, the Data Protection Authority in Indonesia is not yet stipulated.
Japan	Under the APPI, insurance companies who become aware of any of the following incidents, or its likelihood, shall file a preliminary report and a final report to the FSA or other competent authority overseeing business of the insurance company: i. Leakage, loss or damage of sensitive data ii. Leakage, loss or damage of personal data that is likely to cause financial damages if used unlawfully iii. Leakage, loss or damage of personal data that is likely to have been caused by an act committed with a wrongful purpose iv. Leakage, loss or damage of personal data of more than 1,000 data subjects The preliminary report needs to be filed 'swiftly' after insurance companies become aware of the triggering event. 'Swiftly' here is generally understood to mean three to five days, according to the PPC's guidelines. The deadline for filing a final report varies depending on the type of the applicable triggering event. Insurance companies must submit the final reports for (i), (ii) and (iv) within 30 days after becoming aware of the event, and the final report for (iii) must be submitted within 60 days after becoming aware of the event.

		Under the PPC and FSA Guidelines, insurance companies are required to immediately report to the regulators certain data breaches, such as leakage of personal data.
	**Malaysia**	Statutory data breach reporting obligations may be imposed in the future, in view of the public consultation paper published by the Regulator in 2020. For now, there is no express obligation to do so. However, proposed amendments to the PDPA (expected to be tabled at Parliament in 2024) contemplate requiring all data users to report data breaches to the Malaysian Personal Data Protection Department within 72 hours. The Code provides that when data users consider whether there is a need to establish a disaster management plan, it should take into account whether, depending on the severity of the breach, it would be necessary to notify the same to the appropriate authorities, including the Regulator, BNM and police, among others. Further, an insurer is required to complete the investigation of any customer information breach within three months of detecting the same, having regard to the complexity of the breach. The insurer is also required to submit a detailed investigation report containing prescribed information to BNM within one working day upon tabling the same to the board. However, where the customer information breach is likely to pose reputational risk to the insurer or a threat to public confidence and trust, the insurer must notify BNM immediately upon discovery of the breach. There is also a prescribed process for the reporting of customer information breaches.
	**Philippines**	The DPA provides that PICs must notify both the NPC and the affected data subject within 72 hours upon the knowledge or reasonable belief of the PIC that a personal data breach has occurred. Such notification is required under the following conditions: ▪ The personal data involves sensitive personal information or any other information that may, under the circumstances, be used to enable identity fraud. ▪ There is a reason to believe that the information may have been acquired by an unauthorized person. ▪ The PIC or the NPC believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to the affected data subjects. The notification shall include: (a) nature of breach; (b) sensitive personal information involved; and (c) measures taken by the PIC to address the breach.
	**Singapore**	Under the PDPA, the organization must notify the PDPC as soon as practicable, but no less than three calendar days after the day of assessment that a notifiable data breach has occurred. Depending on the nature of the data breach, relevant obligations under the MAS Guidelines on Outsourcing and/or the MAS Notice on Technology Risk Management may also be triggered. The MAS is required to be notified as soon as possible (and within one hour) upon the discovery of any system malfunction or IT security incident that has a severe and widespread impact on the insurer's operations or that materially impacts the insurer's service to its customers. Further provisions in relation to submission of a root cause and impact analysis report are also provided for. In addition, MAS has issued Circular ID 03/23 - Notification of Data Breaches to the Monetary Authority of Singapore, which sets out the expectations for insurers to notify data breaches to MAS; this is, however, not a statutory obligation.
	**Taiwan**	If personal data is stolen, altered, damaged, destroyed or disclosed, insurance companies shall immediately report such event to the FSC. Particularly, if there is any material data breach that would endanger an insurance company's normal operation or would impact the rights and interests of a large number of policyholders, the insurance company should disclose the data breach to the FSC within 72 hours (three calendar days) by filling in the form of the FSC.

		The notification items in the above FSC form include: (a) the time when the data incident occurs; (b) the nature of the data breach; (c) the respective number of the non-sensitive personal data and sensitive personal data involved; (d) a summary of the causes of data breach and the factual background; (e) the extent of damages; (f) the possible consequences of the data breach; and (g) the proposed response plan of this insurance company.
	**Thailand**	If a personal data breach results in a risk to the rights and freedoms of persons, the data controller must notify the Office of the PDP Committee without delay within 72 hours after becoming aware of the incident. If the data breach occurs because of IT failure or cyberattack, the insurer must also report to the OIC.
	**Vietnam**	The short answer is Yes. Data breach is currently regulated under different general and sector-specific regulations. Data breach can be either a personal data violation under the PDPD, a cybersecurity incident or a cyber information security incident respectively per cybersecurity or cyber information security laws, or an attack on the information system that poses a risk to the consumer information's security and safety pursuant to consumer protection regulations, etc. The reporting entity, deadline and procedure also vary across pieces of legislation and subordinates.

22. Is there a statutory obligation to disclose data breaches to data owners?

China	If personal information has been or may be divulged, damaged or lost, network operators shall promptly inform users . Under the Provisions on the Cyber Protection of Personal Information of Children, where there were or are likely to be breaches of children's personal data that caused or may cause any serious consequence, insurance companies shall promptly notify the affected children and their legal custodians by phone, mail, letter or notice. If it is difficult to notify the children and their guardians one by one, the insurer shall publish the relevant warning information by reasonable and effective means.
Hong Kong	No, but the data user should consider notifying data owners where they can be identified.
Indonesia	Yes. The notification must be made within 14 days after the electronic system operator knows about the data breach. The notification must include the reasons and causes of the data breach. The notification can be sent electronically or by email to the data owner(s).
Japan	Yes. Insurance companies which shall file a report to the authority for a data breach shall promptly notify affected individuals of the breach in accordance with the APPI.
Malaysia	No. However, the Regulator may take disclosure to data owners into account in determining compliance with the Security Principle.
Philippines	Yes. Please refer to our response to question 21.
Singapore	Under the PDPA, if a data breach is notifiable, organizations must notify each affected individual as soon as practicable, simultaneously or after notifying the PDPC.
Taiwan	When personal data is stolen, disclosed, altered or violated in any way due to violations of the PDPL, insurance companies shall inform the data subjects (of, for example, the incident background, response plan and a hotline that the data subject can contact) after conducting an investigation.
Thailand	If the personal data breach is likely to result in a significant risk to the rights and freedoms of persons, the data controller shall notify the data subjects about the remedial measures without delay.
Vietnam	Under the Cybersecurity Law, service providers in cyberspace must notify users about any leak, damage or loss of those users' data.

23. What are the statutory obligations to cooperate with regulators if there is a data breach?

China	When the competent authorities perform personal data protection functions, including launching investigations and inspections, consulting, and duplicating the parties' contracts, records, account books and other relevant materials, the parties shall provide assistance and cooperation. When the competent authorities require to hold an interview with the legal representative or primary person in charge of the personal data processor in accordance with the specified authority and procedures, or require the personal data processor to commission a professional institution to audit the regulatory compliance of its or their personal data processing activities, the personal data processor shall adopt measures to make rectification and eliminate hidden risks as required.
Hong Kong	It is not a statutory requirement for data users to inform the PCPD about data breach incidents, but data users are advised to do so as a recommended practice for proper handling of data breaches. In respect of cybersecurity incidents, please refer to our response to question 21 above.
Indonesia	Indonesia's national cybersecurity agency has established a helpdesk that the private sector can consult in cases of data breaches and other incidents (e.g., intrusion, identity theft, hacking and other cybersecurity issues).
Japan	No specific cooperation obligations are provided for in the APPI or the PPC and FSA Guidelines other than those described in questions 21 and 22.
Malaysia	There is no statutory obligation under the PDPA to cooperate with the Regulator in the event of a data breach. However, pursuant to the Management of Customer Information and Permitted Disclosures policy document, in the event of a customer information data breach: ▪ insurers are required to carry out an investigation to ascertain root causes of the breach and determine appropriate remedial actions to prevent future recurrence. Subsequently, a detailed investigation report (in the prescribed form) must be submitted to BNM. ▪ which is likely to pose reputational risk or a threat to public confidence and trust, the breach must be notified to BNM immediately upon discovery of the breach. . which appears to involve fraud, criminal activity or may result in identity theft, insurers must also notify the relevant law enforcement agency.
Philippines	There is no explicit requirement under the DPA to cooperate with the regulators. However, under data privacy regulations, depending on the nature of the incident, or if there is failure or delay in the notification, the NPC may investigate the circumstances surrounding a personal data breach. If necessary, the NPC shall require the cooperation of concerned parties, or compel appropriate action therefrom to protect the interests of data subjects.
Singapore	The PDPC may exercise its enforcement powers in cases of personal data protection breaches, and organizations are required under the PDPA to comply with the directions issued by the PDPC. In this regard, the PDPC may apply for the direction to be registered in a district court and once registered, it shall have the same force and effect for the purposes of enforcement as if it had been an order originally obtained from the district court. For example, under the PDPA, the PDPC may, if it is satisfied that an organization is not complying with any of the data protection provisions, including the protection obligation to keep data safe, give the organization such directions as the PDPC thinks fit in the circumstances to ensure the organization's compliance with that provision.

		The PDPA further provides that the PDPC may give an organization that is not complying with the data protection provisions any or all of the following directions: ▪ To stop collecting, using or disclosing personal data in contravention of the PDPA ▪ To destroy personal data collected in contravention of the PDPA ▪ To comply with any direction of the PDPC issued under the PDPA ▪ To pay a financial penalty of such amount not exceeding SGD 1 million as the PDPC deems fit The MAS may also exercise its powers of regulation over the insurance company.
	**Taiwan**	In the event of a data breach, insurance companies are required to immediately report such event to the FSC, conduct an investigation, and adopt precautionary and remedial measures.
	**Thailand**	The data protection officer has a statutory obligation to cooperate and coordinate with the PDP Committee if there are problems with respect to the collection, use or disclosure of the personal data undertaken by the data controller or data processor. In addition, insurance companies need to cooperate and coordinate with the OIC.
	**Vietnam**	There is a general obligation to cooperate with and support the regulators in resolving data breaches.

24. Is there a publicly accessible cybersecurity assistance service, such as a Computer Emergency Response Team (CERT)?

China	The National Computer Network Emergency Response Technical Team/Coordination Centre (CNCERT/CC) functions as the primary organization for handling computer security incidents and emergencies in China. It is mainly involved in coordinating the response to cybersecurity incidents, monitoring cybersecurity threats, conducting security research, and issuing warnings and guidelines on emerging cybersecurity threats.
Hong Kong	The Hong Kong Police Force's Cyber Security and Technology Crime Bureau, the Hong Kong Computer Emergency Response Team Coordination Centre under the Hong Kong Productivity Council, and the Government Computer Emergency Response Team under the Office of the Government Chief Information Office offer cybersecurity assistance services. In the future, these three organizations/departments may be combined into one to pool resources.
Indonesia	Indonesia's national cybersecurity agency has established a helpdesk that the private sector can consult in cases of data breaches and other incidents (e.g., intrusion, identity theft, hacking and other cybersecurity issues).
Japan	There are cybercrime consultation desks at the police headquarters of each of the prefectural governments.
Malaysia	The Malaysian Computer Emergency Response Team (MyCERT) provides a point of reference for the internet community in Malaysia for dealing with incidents such as intrusion, identity theft, malware infection, cyber harassment and other computer security-related incidents. MyCERT operates, among others, the Cyber999 computer security incident handling and response help center, the Cybersecurity Malaysia Cyber Threat Research Centre, and the Malware Information Sharing Platform. MyCERT works closely with law enforcement agencies such as the police, Securities Commission and BNM.
Philippines	The National Computer Emergency Response Team (NCERT) is a division under the Cybersecurity Bureau of the DICT. NCERT is responsible for receiving, reviewing and responding to computer security incident reports and activities. This division also ensures that systematic information gathering/dissemination, coordination and collaboration among stakeholders, especially computer emergency response teams, are maintained to mitigate information security threats and cybersecurity risks. While not exactly a 'CERT,' the NPC is also mandated under the DPA to provide assistance on matters relating to privacy or data protection, including the enforcement of rights of data subjects, at the request of a national or local agency, a private entity or any person. The NPC may also compel and/or petition any entity, government agency or instrumentality to abide by its orders or take action on a matter affecting data privacy. Queries and complaints may be submitted or filed with the NPC through its website, https://privacy.gov.ph/.
Singapore	The Singapore Computer Emergency Response Team (SingCERT) responds to cybersecurity incidents in Singapore. SingCERT provides technical assistance and coordinates responses to security compromises, identifies trends in hacking activities, and works with other security agencies to resolve computer security incidents. SingCERT also disseminates timely information and alerts on the latest security violation issues to the general public via the SingCERT website and SingCERT mailing list.
Taiwan	The Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC), operated by the National Institute of Cyber Security under the oversight of the Ministry of Digital Affairs, is responsible for responding to cybersecurity incidents in Taiwan. The TWCERT/CC provides technical assistance

		and coordinates responses to cyber security incidents, identifies trends in hacking activities, and works with Taiwan and overseas security agencies to resolve computer security incidents. The TWCERT/CC also disseminates timely information and alerts on the latest security violation issues to the general public via its website.
	**Thailand**	The Thailand Computer Emergency Response Team (ThaiCERT) is a central point of contact that offers assistance to the internet community. The ThaiCERT hears complaints and coordinates with the relevant authorities both in Thailand and abroad to solve computer security issues. The ThaiCERT is under the supervision of the Thai National Cyber Security Agency (NCSA), an organization under the Cybersecurity Act.
	**Vietnam**	The Vietnam Computer Emergency Response Team (VNCERT) is an organization under the MIC that coordinates computer incident responses throughout the country, timely provides warnings about computer network security issues, and encourages the formation of CERT systems in agencies, organizations and enterprises. VNCERT is the local point of contact for working with foreign CERTs.

25. Are there additional consequences that apply in the event of a data privacy breach under cybersecurity laws?

China	Please refer to the response to question 20.
Hong Kong	No, but non-compliance with GL20 may reflect on the Insurance Authority's view of the continued fitness and properness of the directors or controllers of insurance companies.
Indonesia	There are no other regulatory consequences in addition to the criminal and civil offense set out in question 20, but a data privacy breach may result in a loss or modification to the data stored.
Japan	No.
Malaysia	In general, if a data privacy breach is pursuant to acts involving: (a) unauthorized access to a computer with the intent to secure access to any program or data held therein; (b) unauthorized modifications of the contents of any computer; or (c) interception of communications, the person who is found to have committed these acts will be guilty of various offenses in accordance with the Computer Crimes Act 1997 and the Communication and Multimedia Act 1998.
Philippines	Under the Anti-Cybercrime Law, all crimes, including data privacy breaches committed by, through and with the use of information and communications technologies, shall be penalized with a penalty one degree higher than that originally imposed under the law. Moreover, apart from data privacy breaches penalized under the DPA, the Anti-Cybercrime Law also punishes offenses against the confidentiality, integrity and availability of computer data and systems. These include the offenses of: (a) illegal access; (b) illegal interception; (c) data interference; (d) system interference; and (e) misuse of devices.
Singapore	There are criminal sanctions and penalties in computer misuse and cybercrime cases. Under the Computer Misuse Act 1993, there are criminal penalties for cybercrime-related offenses (e.g., unauthorized access to computer material, unauthorized modification of computer material). The Act has extra-territorial scope and applies to any person, whatever their nationality or citizenship, outside as well as within Singapore if, inter alia, the affected computer, program or data was in Singapore at the material time, or if the offense causes or creates a significant risk of serious harm in Singapore. Under the Cybersecurity Act, it is an offence if a prescribed cybersecurity incident is not notified to the commissioner. A fine not exceeding SGD 100,000 and/or imprisonment for a term not exceeding two years may be imposed.
Taiwan	Under cybersecurity laws, if a cyber security incident involves personal data leakage, the PDPL, which has harsher penalties for data privacy breaches, will apply first. Please refer to the possible consequences set out in the response to question 20. Additionally, offenders will face criminal liabilities if a data privacy breach involves offenses set out in the Criminal Code, for instance: (a) a person who, without reason, by entering another's account code and password, breaking their computer protection or taking advantage of the system loophole of such other, accesses the computer or related equipment; (b) a person who, without reason, obtains, deletes or alters the magnetic record of another's computer or related equipment and causes injury to the public or others; and (c) a person who, without reason, interferes, through the use of computer programs or other electromagnetic

		methods, with the computer or related equipment of another person and causes injury to the public or another.
	**Thailand**	If an insurance company commits a personal data breach that affects or poses a risk to its services or the implementation of computer networks or the internet, such that it may compromise the national, economic, financial or commercial stability of the nation, the NCSC may order that insurance company to take or cease from taking any action to facilitate the committee, submit any account, document, or evidence for the purpose of inspection and investigation.
	**Vietnam**	Under cybersecurity laws, failure of a foreign enterprise providing certain cyberspace services to cooperate with a competent authority in handling a cybersecurity violation, which can encompass a data privacy breach, is one of the elements triggering the data localization and local branch / representative office establishment obligations.

For more information about this guide, please contact:

China

Ada Hu
Partner
+86 10 5649 6080
huguangjian
@fenxunlaw.com

Hong Kong

Martin Tam
Partner
+852 2846 1629
martin.tam
@bakermckenzie.com

Indonesia

Gerrit Jan Kleute
Partner
+65 6434 2315
gerrit.kleute
@bakermckenzie.com

Japan

Satoshi Abe
Partner
+81 3 6271 9490
satoshi.abe
@bakermckenzie.com

Malaysia

Sue Wan Wong
Partner
+603 2298 7884
suewan.wong
@wongpartners.com

Philippines

Charles Veloso
Partner
+63 2 8819 4954
charles.veloso
@quisumbingtorres.com

Singapore

Stephanie Magnus
Principal
+65 6434 2672
stephanie.magnus
@bakermckenzie.com

Taiwan

Hao-Ray Hu
Partner
+886 2 2715 7281
hao-ray.hu
@bakermckenzie.com

Thailand

Sivapong Viriyabusaya
Partner
+66 26662824 #4041
sivapong.viriyabusaya
@bakermckenzie.com

Vietnam

Thanh Hai Nguyen
Partner
+84 24 3936 9606
thanhhai.nguyen
@bakermckenzie.com

Baker McKenzie delivers integrated solutions to complex challenges.

Complex business challenges require an integrated response across different markets, sectors and areas of law. Baker McKenzie's client solutions provide seamless advice, underpinned by deep practice and sector expertise, as well as first-rate local market knowledge. Across more than 70 offices globally, Baker McKenzie works alongside our clients to deliver solutions for a connected world.

bakermckenzie.com