



**Baker
McKenzie.**

2020

Asia Pacific Guide for Insurance Data Protection and Cybersecurity

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, 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 arise.














CONTENTS







Regulatory environment

1. Who is the main regulator with oversight of data privacy matters?
2. What is the main legislation on the protection of personal data privacy?
3. Who is the main regulator with oversight of cyber security matters?
4. Is there existing legislation governing cyber security issues?






WHO IS THE MAIN REGULATOR WITH OVERSIGHT OF DATA PRIVACY MATTERS?

 AUSTRALIA	The Office of the Australian Information Commissioner (OAIC)
 CHINA	There is no specific data privacy regulator in China. However, following the issuance of the PRC Cybersecurity Law and other data protection laws, the Cybersecurity Administration of China (CAC) and the Ministry of Public Security (MPS) — together with relevant industrial regulators (in the case of insurance companies, the China Banking and Insurance Regulatory Commission or CBIRC) — 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 no specific data privacy regulator in Indonesia. Multiple government agencies are involved. While the Ministry of Communication and Informatics has overall responsibility for data privacy, the government authority for financial institutions (including insurance companies) is the Financial Services Authority (OJK).
 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). With respect to data-privacy-related regulations of the Philippine Insurance Code and regulations issued by the Philippine Insurance Commission (IC), the same are administered by the IC.
 SINGAPORE	The Personal Data Protection Commission (PDPC).
 TAIWAN	The Insurance Bureau, Financial Supervisory Commission (FSC) is the personal data protection regulator for insurance enterprises.
 THAILAND	The Personal Data Protection Committee (PDP Committee), which has yet to be set up
 VIETNAM	There is no designated data privacy regulator as Vietnam has not passed a consolidated data privacy law. However, the Ministry of Information and Communications (MIC) is the government body charged to regulate matters that would include data privacy.












WHAT IS THE MAIN LEGISLATION ON THE PROTECTION OF PERSONAL DATA PRIVACY?

	AUSTRALIA	Privacy Act 1988 (Cth)
	CHINA	There is no specific data privacy legislation in China, but the concept and general requirements can be found in laws and regulations, such as in the General Rules of Civil Code, the Cybersecurity Law, the Tortious Liability Law, the Criminal Law, the NPC Decision on Strengthening the Protection of Network Information, the Consumer Protection Law, and the Provisions on the Cyber Protection of Personal Information of Children.
	HONG KONG	Personal Data (Privacy) Ordinance (Cap. 486) (PDPO)
	INDONESIA	The main regulation is 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 (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 Industries in Malaysia (Code), which came into effect on 23 December 2016, should be read together with the PDPA.












WHAT IS THE MAIN LEGISLATION ON THE PROTECTION OF PERSONAL DATA PRIVACY?

 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	Personal Data Protection Act 2012 (PDPA)
 TAIWAN	The Personal Data Protection Law (PDPL)
 THAILAND	The Personal Data Protection Act 2019 (PDPA); however, most of the key provisions will become effective on 27 May 2020. Accordingly, the most relevant laws relating to data privacy available at the moment would be the Constitution of the Kingdom of Thailand 2017 and the law of Wrongful Act (Tort) provided under the Civil and Commercial Code of Thailand (CCC).
 VIETNAM	There is no consolidated law that addresses the protection of personal data privacy. The concept exists under various laws and regulations, including the Constitution, the Civil/Criminal Code, the Law on Protection of Consumers' Rights, the Law on E-Commerce, the Law on Information Technology, the Law on Insurance Business, the Law on Credit Institutions, the Law on Network Information Security, and the recently passed Cybersecurity Law. Primary legislation is broad while implementing regulations (when they exist) tend to be more specific.

WHO IS THE MAIN REGULATOR WITH OVERSIGHT OF CYBERSECURITY MATTERS?

 AUSTRALIA	<p>There is no particular regulator tasked with oversight of cybersecurity matters per se. The OAIC is the relevant regulator if personal data is involved.</p> <p>The Australian Prudential Regulatory Authority (APRA), the regulator that oversees banks, other financial institutions and insurance industries, provides a set of standards/guidelines in relation to IT security, which applies to, among other institutions, the general insurance, life insurance and superannuation industries.</p> <p>The Australian Securities and Investments Commission (ASIC) may also have some oversight of cybersecurity matters in the insurance industry.</p>
 CHINA	<p>CAC and MPS</p>
 HONG KONG	<p>There is no specific regulator. For insurance companies, the Insurance Authority remains the main regulator.</p>
 INDONESIA	<p>The Ministry of Communication and Informatics</p>
 JAPAN	<p>The Cybersecurity Strategic Headquarters and the National Center of Incident Readiness and Strategy for Cybersecurity</p>
 MALAYSIA	<p>The Malaysian Communications and Multimedia Commission and CyberSecurity Malaysia</p>
 PHILIPPINES	<p>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).</p>
 SINGAPORE	<p>The Cyber Security Agency of Singapore (CSA)</p>
 TAIWAN	<p>The Ministry of Justice</p>
 THAILAND	<p>The National Cyber Security Committee (NCSC)</p>
 VIETNAM	<p>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, the Ministry of National Defense, 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.</p>

IS THERE EXISTING LEGISLATION GOVERNING CYBERSECURITY ISSUES?

 AUSTRALIA	The Privacy Act, which governs personal information; Cybercrime Act 2001; Australian Security Intelligence Organisation (ASIO) Act 1979; Telecommunications (Interception & Access) Act 1979; Telecommunications Act 1997; Spam Act 2003; Security of Critical Infrastructure Act 2018
 CHINA	The Cybersecurity Law that came into effect on 1 June 2017, and the implementation regulations, rules and guidelines to be issued in accordance with the Cybersecurity Law
 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. Law No. 11 of 2008 on Electronic Information and Transactions, as amended by Law No. 19 of 2016 (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 Communication and Multimedia Act 1998. Further, the Central Bank of Malaysia (BNM) has issued the Risk Management in Technology (RMIT) policy document, which is specific to financial institutions (such as insurers), wherein they are required 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.
 SINGAPORE	Computer Misuse Act (Cap. 50A) and Cybersecurity Act (No. 9 of 2018)
 TAIWAN	Aside from the PDPL, Chapter 36 of the Criminal Code 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?
6. What are the main requirements for ensuring security of personal data?
7. Are there additional requirements with respect to "sensitive personal data"?
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?
9. Are insurance companies required to have a data protection officer?
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?
11. What are data subjects' rights, if any, in relation to the processing of their personal data?

WHAT ARE THE MAIN REQUIREMENTS WITH RESPECT TO COLLECTION, USE, DISCLOSURE OR TRANSFER OF PERSONAL DATA?



AUSTRALIA

An insurer handling personal information should follow the Australian Privacy Principles (APPs) below:

- Open and transparent management of personal information – All entities subject to the Privacy Act must have an APP Privacy Policy.
- Anonymity and pseudonymity – Individuals should have the option of not identifying themselves when dealing with an organization, unless this is impracticable or the organization is required by law to deal with an individual on an identified basis.
- Collection of solicited personal information – An organization must not collect personal information unless reasonably necessary for one or more of the entity's functions or activities.
- Dealing with unsolicited information – An organization must take specific steps if it obtains personal information that it did not specifically solicit.
- Notification – Individuals must be provided with a collection statement before or at the time their information is collected.
- Disclosure for a primary purpose – Use or disclosure of personal information is not permitted for purposes other than the primary purpose for which it was collected.
- Direct marketing – Subject to exceptions, use or disclosure of personal information for direct marketing purposes is not permitted without consent.
- Cross-border disclosure of personal information – Entities are required to take reasonable steps to ensure that an overseas recipient of Australian personal information does not breach the APPs, and such entity will remain liable for any misuse by the overseas recipient.
- Integrity of personal information – An organization may not adopt a government-related identifier (such as a tax file number) as its own identifier.
- Quality of personal information – An organization must take reasonable steps to ensure that personal information it collects, uses or discloses is accurate, up to date and complete.
- Security of personal information – An organization must take reasonable steps to protect personal information it holds from misuse, interference and loss as well as from unauthorized access, modification or disclosure.
- Access to personal information – Individuals have a right to access their personal information on request.
- Correction of personal information – Organizations must take reasonable steps to correct personal information on request by an individual.





CHINA

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. The legal custodians' consent for the collection, use, transfer and disclosure of personal data of children under 14 must also be obtained.

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 a security assessment conducted by Chinese regulators.

WHAT ARE THE MAIN REQUIREMENTS WITH RESPECT TO COLLECTION, USE, DISCLOSURE OR TRANSFER OF PERSONAL DATA?

 HONG KONG	<p>An insurer (that is, a data user) handling personal data should follow the six data protection principles (DPPs) below:</p> <ul style="list-style-type: none"> · 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 fulfillment of the purposes for which the data is used. · Use of personal data – Unless prior “prescribed consent” has been obtained from the data subject (for example, 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	<ul style="list-style-type: none"> · Consent – The private data owner must give consent to the collection and utilization of private data. The consent must be in writing, which makes it express and opt-in consent. The consent is also for a specific purpose. A ‘blanket’ consent is no longer recognized as valid. · 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 after coordinating with the Ministry of Communication and Informatics. · Data breach – Electronic system operators are required to promptly notify the data owners in writing when there is a data breach. The notification must include the reasons for or causes of the data breach. The notification can be sent through electronic means, e.g., email. · Right to be forgotten – The data owner has the right to request his/her 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.

WHAT ARE THE MAIN REQUIREMENTS WITH RESPECT TO COLLECTION, USE, DISCLOSURE OR TRANSFER OF PERSONAL DATA?



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.
- 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 (that is, 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.

WHAT ARE THE MAIN REQUIREMENTS WITH RESPECT TO COLLECTION, USE, DISCLOSURE OR TRANSFER OF PERSONAL 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 his/her consent for the processing of his/her 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, amongst others:



MALAYSIA

- 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.

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:



PHILIPPINES

- 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 fulfill 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 instruct another to collect, hold, process, use, transfer or disclose personal information on its/his/her behalf.
- The processing is necessary to protect vitally important interests of the data subject (for example, 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 fulfill 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.

WHAT ARE THE MAIN REQUIREMENTS WITH RESPECT TO COLLECTION, USE, DISCLOSURE OR TRANSFER OF PERSONAL DATA?



PHILIPPINES

Moreover, in principle, the processing of personal information must comply with the three basic principles of (a) transparency, (b) legitimacy of purpose, and (c) 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 his or her personal data, including the risks and safeguards involved, his or her rights as a 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 nine key obligations:

- 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 his/her 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 his/her request.
- Accuracy – make reasonable effort 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 – 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.
- Openness – 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 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 data protection obligation and the data retention limitation obligation.

WHAT ARE THE MAIN REQUIREMENTS WITH RESPECT TO COLLECTION, USE, DISCLOSURE OR TRANSFER OF PERSONAL DATA?

 TAIWAN	<p>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.</p> <p>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.</p>
 THAILAND	<p>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.</p> <p>Exceptions to consent for general personal data include the following:</p> <ol style="list-style-type: none"> (1) It is for the achievement of the 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 his or her personal data. (6) It is necessary for compliance with a law to which the data controller is subject. <p>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, unless:</p> <ol style="list-style-type: none"> (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. <p>The collection of personal data shall be limited to the extent necessary in relation to the lawful purpose of the data controller.</p> <p>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 to be 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).</p>






WHAT ARE THE MAIN REQUIREMENTS WITH RESPECT TO COLLECTION, USE, DISCLOSURE OR TRANSFER OF PERSONAL DATA?



VIETNAM

There is no consolidated data privacy law that specifies the main requirements with respect to collection, use, disclosure or transfer of personal data. Generally, however, a data custodian (which may include an insurer) that collects, processes, and uses the personal data of another party must obtain consent from the data subject. The data custodian must: (i) provide notice of the form, scope, place and purpose of the collection/processing/use of the personal data; (ii) use the data for proper purposes and store it only as long as legally required or as agreed upon; (iii) take necessary measures to ensure safety of the data; (iv) allow or enable updates to the data when the data custodian is aware or informed that it is inaccurate; and (v) not use that data until corrected. A data custodian may not transfer personal data to a third party without the data subject's consent, unless otherwise authorized by law.

WHAT ARE THE MAIN REQUIREMENTS FOR ENSURING SECURITY OF PERSONAL DATA?

 AUSTRALIA	<p>Under APP 11, an APP entity must take active measures to ensure the security of personal information it holds, and to actively consider whether it is permitted to retain personal information. An APP entity that holds personal information must do the following:</p> <ul style="list-style-type: none"> · Take reasonable steps to protect the information from misuse, interference and loss, as well as unauthorized access, modification or disclosure. · Take reasonable steps to destroy or de-identify the personal information it holds once the personal information is no longer needed for any purpose for which the personal information may be used or disclosed under the APPs.
 CHINA	<ul style="list-style-type: none"> · Keep the personal data collected strictly confidential, and do not disclose, tamper with, damage, sell or unlawfully provide the same to a third party. · Adopt technical and other necessary measures to ensure that data is secure, and take remedial steps immediately where data disclosure, damage or loss occurs or may occur. Network operators shall fulfill 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	<p>Data users must take all practicable steps to ensure that personal data is protected against unauthorized or accidental access, processing, erasure or other use.</p>
 INDONESIA	<p>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.</p>
 JAPAN	<p>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.</p>

WHAT ARE THE MAIN REQUIREMENTS FOR ENSURING SECURITY OF PERSONAL DATA?



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, amongst others:

- Deploying preventive and detective information and communication technology controls to prevent theft, loss, misuse, unauthorized access, disclosure or modification of customer information and 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 which 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.

WHAT ARE THE MAIN REQUIREMENTS FOR ENSURING SECURITY OF PERSONAL DATA?

	PHILIPPINES	<ul style="list-style-type: none"> 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. <p>PICs must ensure that PIPs or third-party subcontractors also implement the foregoing measures.</p>
	SINGAPORE	Organizations are required to implement appropriate 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, for example, taking into consideration the nature of personal data, the form in which the personal data has been collected (for example, electronic or physical) and the possible impact to the individual concerned if an unauthorized person obtains, modifies or disposes of the personal data.
	TAIWAN	Data collectors shall take appropriate security measures to prevent personal data from being stolen, altered, damaged, destroyed or disclosed and 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	Personal data should be kept confidential and not be disclosed unless authorized either by law or the data subject. A data custodian must take necessary technical and managerial measures to ensure personal data is not lost, stolen, disclosed, modified or destroyed.

ARE THERE ADDITIONAL REQUIREMENTS WITH RESPECT TO “SENSITIVE PERSONAL DATA”?



AUSTRALIA

“Sensitive information” is defined in the Privacy Act as personal information relating to racial or ethnic origin; political opinions; membership in a political association, professional or trade association or trade union; religious beliefs or affiliations; philosophical beliefs; sexual preferences or practices; criminal record; biometric information; or health information. Pursuant to APP 3, an entity must not collect sensitive information unless:

- The entity obtains the consent of the individual and the information is reasonable necessary for the activities or functions of the entity.
- Collection is required by law.
- Collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where it is unreasonable or impracticable to obtain the consent of the individual to whom the information relates.
- The information is collected by a nonprofit organization and relates solely to the organization’s activities and to the organization’s members or persons who have regular contact with the organization in connection with its activities.
- Collection is necessary for the establishment, exercise or defense of a legal or equitable claim.
- Where the entity is a Commonwealth enforcement body, the collection is necessary for the performance of that enforcement body’s functions or activities.
- The information is collected in the process of providing a health service, and is either collected as authorized by law or subject to a professional code of ethics.
- The information is collected in the course of medical research that is subject to professional safeguards and where obtaining consent is impracticable, and the research cannot be performed without the information being collected.

Unless consent is given for an additional use, sensitive information may only be used for the purpose for which it was collected or for a secondary purpose directly related to the purpose of its collection for which the individual would reasonably expect the information to be used.

Sensitive information is subject to additional and special consent requirements. In non-binding guidelines, the Privacy Commissioner expressed the view that an entity would ordinarily need clear evidence that an individual had consented to it collecting sensitive information.







CHINA




The Information Security Technology – Personal Information Security Specification (GB/T 35273-2017) sets out recommended best practices with respect to sensitive personal data. For instance, specific, clear and explicit consent (on a fully informed and voluntary basis) should be obtained when collecting sensitive personal data, and security measures (such as encryption) should be taken for storage and transfer of sensitive personal data.

Under the draft Administrative Measures for Data Security, where a network operator collects sensitive personal data for business purpose, it shall designate the personnel responsible for data security and file records with the local cyberspace administration.

ARE THERE ADDITIONAL REQUIREMENTS WITH RESPECT TO “SENSITIVE PERSONAL DATA”?

 HONG KONG	<p>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.</p>
 INDONESIA	<p>There is no distinction between general personal data and sensitive personal data and consequently no difference in their treatment. However, as an update, the Indonesian government is working on a draft data privacy law that may include the concept of sensitive personal data.</p>
 JAPAN	<p>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.</p> <p>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.</p>
 MALAYSIA	<p>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.</p> <p>An insurer is also required by BNM to amongst others:</p> <ul style="list-style-type: none"> · 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 · Adopt prescribed controls or their equivalent to secure the storage and transportation of sensitive data in removable media, such as: <ul style="list-style-type: none"> - Implementing authorized access control to sensitive data (e.g., password protection) - Deploying the latest industry-tested and accepted encryption techniques.

ARE THERE ADDITIONAL REQUIREMENTS WITH RESPECT TO “SENSITIVE PERSONAL DATA”?

 PHILIPPINES	<p>With respect to the required consent to the processing of personal information, 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.</p> <p>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 when:</p> <ul style="list-style-type: none"> · The data subject has given his or her 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.
 SINGAPORE	<p>There are no specific requirements for sensitive personal data. However, 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 such sensitive personal data, such concerns are likely to be addressed in sector-specific laws that apply concurrently. The Monetary Authority of Singapore (MAS) expects financial institutions 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. Financial institutions must conduct regular security reviews and tests to ascertain the continued effectiveness of these measures.</p>
 TAIWAN	<p>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. However, if an insurance company obtains the data subject's written consent, such company will be allowed to collect, process and use the data subject's personal data in connection with his or her 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).</p>

ARE THERE ADDITIONAL REQUIREMENTS WITH RESPECT TO “SENSITIVE PERSONAL DATA”?

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 of 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 where:

- (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 by 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:
 - (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.



THAILAND

ARE THERE ADDITIONAL REQUIREMENTS WITH RESPECT TO “SENSITIVE PERSONAL DATA”?









VIETNAM

Sensitive data may include data that harms the interests of the state/government of Vietnam or causes social instability. Personal data relating to religious or other beliefs or political opinions, for instance, may also be regarded as sensitive, the production, reproduction, access and dissemination of which is prohibited.




The concept of “personal secrets” also exists under Vietnamese law, and is defined as: medical records, tax payment dossiers, social insurance card numbers, credit card numbers, and others as defined by law. State agencies holding information classified as personal secrets may only supply or share such information with a competent third party in cases specified by law.

If the sensitive data relates to state secrets, the information must be encrypted in network transmission and computer storage.



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?

 AUSTRALIA	<p>Insurance companies that are APP entities must comply with their obligations under the Privacy Act as set out in response to questions 5 to 7 above. There are no particular registration requirements to be complied with.</p>
 CHINA	<p>Requirements are discussed in question 5.</p> <p>There are, however, 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.</p> <p>In addition, 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.</p>
 HONG KONG	<p>The main requirements set out in question 3 are applicable to insurance companies.</p> <p>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 (for example, 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, etc.</p>
 INDONESIA	<p>The main requirements set out in question 5 are applicable to insurance companies.</p>
 JAPAN	<p>The main requirements set out in question 5 are applicable to insurance companies.</p> <p>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.</p>
 MALAYSIA	<p>The main requirements set out in our response to question 5 are applicable to insurance companies.</p> <p>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.</p> <p>In addition, insurers must also be registered with the Regulator pursuant to the PDPA.</p> <p>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.</p>







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?

 PHILIPPINES	<p>The requirements as discussed above are applicable to insurance companies, as they fall under the definition of PICs.</p> <p>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:</p> <ul style="list-style-type: none"> · it has at least 250 employees; or · it processes the sensitive personal information of at least 1,000 data subjects; or · it is processing personal data on a regular basis; or · it is processing personal data that is likely to pose a risk to the rights and freedoms of the data subjects. <p>Specifically, insurance companies (among others) have been identified under NPC Circular No. 2017-01 as among the sectors/institutions covered by the mandatory registration requirements.</p> <p>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.</p> <p>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.</p>
 SINGAPORE	<p>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 as well.</p>
 TAIWAN	<p>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 data subject. With respect to non-sensitive personal data, consent does not have to be a written consent; however, it is suggested to obtain written consent for evidentiary purpose.</p>






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?

 THAILAND	<p>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 (detailed in question 5 and 7).</p> <p>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 notify the data subject of the required details before or at the time of such collection, except in the case 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, etc.).</p>
 VIETNAM	<p>Aside from the general obligations regarding the collection, use, and transfer of personal data (see question 5 above), there is no specific obligation on insurance companies regarding the use and transfer of personal data.</p>








ARE INSURANCE COMPANIES REQUIRED TO HAVE A DATA PROTECTION OFFICER?

 AUSTRALIA	<p>In Australia, although it is considered best practice to do so, there is no legal requirement to appoint or designate a data privacy officer. However, organizations are required to make available a privacy policy on request from a data subject.</p>
 CHINA	<p>No. However, 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 35273-2017).</p>
 HONG KONG	<p>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.</p>
 INDONESIA	<p>No. However, insurance companies are 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. The general responsibility sits with insurance companies' board of directors that are required to conduct a risk assessment of the data management system utilized by insurance companies to ensure the reliability of the data management system.</p>
 JAPAN	<p>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.</p>
 MALAYSIA	<p>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 on-going 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 (by whatever name called) to be responsible for the technology risk management function of the insurer.</p>





ARE INSURANCE COMPANIES REQUIRED TO HAVE A DATA PROTECTION OFFICER?

 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	All organizations are required to designate at least one person (a Data Protection Officer) to be responsible for ensuring that the organization complies with the PDPA, such as developing personal data policies for the organization’s compliance 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 his/her 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	Insurance companies are not required to have a data protection officer.

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?

 AUSTRALIA	<p>While not a strict legal requirement, APP 1 requires APP entities to take reasonable steps to implement practices, procedures and systems that will ensure compliance with the APPs and enable them to deal with enquiries or complaints about privacy compliance. In this way, the APPs require “privacy by design,” an approach whereby privacy compliance is designed into projects dealing with personal information right from the start, rather than being bolted on afterward. Conducting privacy impact assessments (PIAs) helps entities ensure privacy compliance and identify better practice.</p> <p>OAIC guidelines recommend and provide guidance for conducting PIAs for “projects” such as the implementation of new or amended programs, activities, systems or databases. A project that conducts a PIA will undergo a systemic assessment in order to understand the impact it has on the privacy of the individual. After the systemic assessment is completed, recommendations for managing, minimizing or eliminating impacts on privacy should be identified. In the event a project changes, a PIA should be revisited and updated so it can evolve alongside the project. Similarly, conducting PIAs would assist in complying with APRA standards surrounding cybersecurity and managing data risk.</p>
 CHINA	<p>Current rules do not specifically provide that privacy impact assessments must be conducted. However, according to applicable rules, insurance companies are required to undertake various security assessments before implementing new information systems and/or technologies. Hence, it is reasonable to expect that privacy or data security assessments should be conducted as part of the assessment.</p> <p>In addition, the CAC is in the process of formulating the guidelines on privacy impact assessment. Once the guidelines are finalized, it is expected that companies in China, including insurance companies licensed in China, will need to conduct privacy impact assessments accordingly.</p>
 HONG KONG	<p>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.</p>
 INDONESIA	<p>Privacy impact assessments are not required per se. However, the board of directors is required to conduct a risk assessment of the data management system utilized by insurance companies to ensure the reliability of the data management system.</p>
 JAPAN	<p>Privacy impact assessments are not expressly required.</p>
 MALAYSIA	<p>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. Where new information systems and/or technologies are implemented in connection with the offering of internet insurance services for the first time, an insurer is required to submit prescribed notifications to BNM.</p>
 PHILIPPINES	<p>Privacy impact assessments (PIAs) are not expressly required under the DPA. However, the conduct of PIAs is recommended to ensure the security of processing of personal data. In fact, under Circular No. 16-03 issued by the NPC – the government agency tasked with implementing the provisions of the DPA – conducting a PIA is one of the identified safeguards intended to prevent or minimize the occurrence of personal data breaches.</p>

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?

 SINGAPORE	Privacy impact assessments are not specifically required. However, technical and other necessary measures are recommended to ensure that the data is secure. 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 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	Insurance companies are not specifically required to undertake privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of personal data.

**AUSTRALIA**

Data subjects have the general right to:

- Be informed by an organization of the personal data the organization holds about the data subject
- Access the data subject's personal data, subject to some restrictions and/or qualifications
- Request the correction of the data subject's personal data
- Request the deletion and/or destruction of the data subject's personal data.

Australia is also introducing the so-called "consumer data right", which will provide consumers with access to data about their accounts in certain sectors (which currently is proposed to include data from the banking, energy and telecommunications sectors) and enables them to share such data with accredited third-party recipients.

**CHINA**

When a data subject finds that his/her personal data has been collected or used in breach of applicable laws and regulations or the agreement with the data collector, he/she has the right to request the data collector to delete his/her personal data. If a data subject finds that the personal data collected or stored by a network operator (such as an insurance company) contains an error, he/she can request the network operator to correct or delete the relevant data.

**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.




**INDONESIA**

Data subjects have the right to:

- Access their personal data
- Correct their personal data
- Deem personal data to be treated as confidential information
- Access historical information on personal data that has been collected
- Withdraw, revoke or amend consents previously given
- Be forgotten
- File claims with the data user if the data user fails to perform its obligation, e.g., maintain the secrecy of the data.

 JAPAN	<p>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.</p> <p>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.</p> <p>If a data subject requests disclosure of his/her information or modifications to his/her information, the business operator must, in principle, comply with such requests unless:</p> <ul style="list-style-type: none"> · 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	<p>In general and subject to certain prescribed exceptions, data subjects have the following rights:</p> <ul style="list-style-type: none"> · 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 his/her 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	<p>Under the DPA, data subjects have the following rights:</p> <ul style="list-style-type: none"> · 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 which is being processed and other relevant information thereon (such as the sources thereof, names and addresses of the recipients, reasons for disclosure, etc.) · 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 his or her 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.
 SINGAPORE	<p>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:</p> <ul style="list-style-type: none"> · 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.

 SINGAPORE	<p>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:</p> <ul style="list-style-type: none"> · A reasonable person would consider appropriate in the circumstances · Where applicable, that the data subject has been informed of by the organization. <p>In addition to the above, the PDPC is proposing a Data Portability Obligation, which allows individuals to request an organization to move certain data of the individual to another organization.</p>
 TAIWAN	<p>According to Article 3 of the PDPL, the following rights should be exercised by the data subject with regard to his or her personal information and should not be waived in advance or limited by a specific agreement:</p> <ul style="list-style-type: none"> · 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	<p>Under PDPA, data subjects have certain rights such as:</p> <ul style="list-style-type: none"> · 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, i.e., 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 or destroy the personal data, or anonymize the 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 remains accurate, up-to-date, complete, and not misleading · Right to file a complaint with the competent authority.







WHAT ARE DATA SUBJECTS' RIGHTS, IF ANY, IN RELATION TO THE PROCESSING OF THEIR PERSONAL DATA?**VIETNAM**

A data subject has the right to require a data custodian to provide their personal data to them. A data subject may require a data custodian to amend, update and/or delete any personal data in their possession. Upon receipt of such request, the data custodian must amend or delete the relevant personal data. In addition, if a third-party transfer occurs pursuant to the data subject's consent, the data subject may revoke consent and require the data custodian to stop the third-party transfer. Upon such request, the data custodian must comply and notify the data subject of such compliance.




Data transfer and outsourcing

12. Are there any restrictions regarding cross-border transfers of personal data for insurance companies?
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?
14. Are there any specific requirements for insurance companies in relation to the receipt of personal data from their business partners?
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?
16. Are there additional requirements imposed with respect to the outsourcing of data processing to third-party data processors?
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?

ARE THERE ANY RESTRICTIONS REGARDING CROSS-BORDER TRANSFERS OF PERSONAL DATA FOR INSURANCE COMPANIES?

 AUSTRALIA	<p>If an insurance company discloses personal data to a recipient outside of Australia, it must take reasonable steps to ensure that the offshore recipient (including a related entity) does not breach the APPs. Unless an exception applies, if the recipient handles the personal data in a manner that would breach the APPs if that recipient were subject to the APPs, the organization that disclosed the information will be taken to have breached the APPs.</p> <p>A key exception is if the recipient to which personal data is disclosed is subject to a law or binding scheme that provides the same protection as under the Privacy Act, and there are mechanisms that the data subject can access to enforce that law or binding scheme. A further exception is if the organization expressly informs data subjects that if information is disclosed outside of Australia, the organization will not be responsible for any failure of the recipient to protect the personal data in a manner consistent with the APPs, and having been so informed, the data subject consents to the disclosure.</p>
 CHINA	<p>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.</p>
 HONG KONG	<p>The transfer of data outside of Hong Kong is restricted under the PDPO, though this restriction is not yet effective.</p>
 INDONESIA	<p>Consent from data owner is required. In addition, in theory insurance companies must coordinate with the Ministry of Communication and Informatics 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 implemented given the absence of implementing guidelines from the Ministry of Communication and Informatics.</p> <p>Further, insurance companies must store certain personal data in data centers situated in Indonesia. The data being transferred should only comprise copies (mirroring).</p>
 JAPAN	<p>The APPI provides that personal data may not be transferred to a foreign country unless: (a) the data subject has given specific advance 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 have been designated as countries that have a legal system deemed equivalent to the Japanese personal data protection system.</p>
 MALAYSIA	<p>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 in the event that the personal data is being stored or processed by a third party / outsourcing party.</p>

ARE THERE ANY RESTRICTIONS REGARDING CROSS-BORDER TRANSFERS OF PERSONAL DATA FOR INSURANCE COMPANIES?

 PHILIPPINES	<p>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”.</p> <p>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.</p> <p>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.</p>
 SINGAPORE	<p>An organization should obtain express opt-in consent for the use and disclosure of personal data for marketing purposes. 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.</p>
 TAIWAN	<p>Processing and use of personal data internationally by insurance companies are subject to the PDPL.</p> <p>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.</p> <p>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.</p>

ARE THERE ANY RESTRICTIONS REGARDING CROSS-BORDER TRANSFERS OF PERSONAL DATA FOR INSURANCE COMPANIES?



THAILAND

The PDPA specifies that if personal data is transferred to other countries, the data controller must comply with a sub-regulation to be issued by the PDP Committee and the destination countries or international organization must have adequate personal data protection standards, except where:

- (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 other 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, 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

There are no specific restrictions regarding the cross-border transfer of personal data.








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?

	AUSTRALIA	<p>Whether businesses can use personal data for direct marketing will depend on how they collected the information (whether it was directly from the relevant data subject or from a third party) and whether individuals would reasonably expect their information to be used for this purpose). There is also an opt-out requirement that applies to all direct marketing communications. Additional restrictions apply to the use of Sensitive Data for direct marketing.</p> <p>In addition to requirements under the Privacy Act, direct marketing communications are also subject to requirements under the Spam Act 2003, which prohibits the sending of electronic commercial messages without consent and requires all such messages to contain certain information and an unsubscribe facility. The Do Not Call Register Act 2006 prohibits businesses from contacting individuals on the Do Not Call Register by telephone or fax except in certain restricted circumstances. To the extent the Spam Act or the Do Not Call Register Act applies, the Privacy Act does not apply.</p>
	CHINA	<p>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.</p>
	HONG KONG	<p>A data user (for example, 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.</p> <p>If an insurer intends to use the personal data of its customers in direct marketing, it must inform the customers of its intention to so use the data. Certain prescribed information must be provided to the customers. A response channel (for example, a telephone hotline) must be provided so that the customers may, without charge, communicate their consent to the intended use through such response channel.</p>
	INDONESIA	<p>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.</p>
	JAPAN	<p>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 named 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.</p>
	MALAYSIA	<p>An insurer (that is, 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 the opportunity to choose not to receive such communications or subsequent marketing messages.</p> <p>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.</p>





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?

 PHILIPPINES	<p>Generally, with respect to the use by PICs or PIPs 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 his/her personal data, including, where applicable, the processing of his/her personal data for purposes of direct marketing. Moreover, when data is shared by a PIC/PIP to third parties for purposes of direct marketing (or any other commercial purpose), the DPA requires that there be an express “data-sharing agreement” between the PIC/PIP and the third party to whom such data is shared. Such “data-sharing agreement” (a) must establish adequate safeguards for data privacy and security and must uphold the rights of the data subjects, and (b) will be subject to review by the NPC, on the latter’s initiative or upon complaint of a data subject.</p> <p>In addition, IC Circular Letter No. 2014-47 provides for the following rules regarding the use of client/customer information for marketing purposes:</p> <ul style="list-style-type: none"> · 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	<p>An organization should obtain express opt-in consent for the use and disclosure of personal data for marketing purposes. 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.</p>
 TAIWAN	<p>Joint promotion – Disclosure, transfer or exchange of clients’ personal data shall require prior consent (written consent is recommended for evidentiary purposes).</p> <p>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.</p> <p>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 his/her consent.</p> <p>TV marketing –The PDPL applies to the sale of insurance products on TV.</p>
 THAILAND	<p>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.</p>
 VIETNAM	<p>Aside from the general obligations regarding the collection, use, and transfer of personal data, no specific obligations on insurance companies exist regarding the use and transfer of personal data for marketing purposes. However, please note that spam laws prevent a business operator from sending marketing emails/messages to a party without their prior consent.</p>









ARE THERE ANY SPECIFIC REQUIREMENTS FOR INSURANCE COMPANIES IN RELATION TO THE RECEIPT OF PERSONAL DATA FROM THEIR BUSINESS PARTNERS?

 AUSTRALIA	<p>Where personal data other than sensitive data is collected from a third party, an insurance company may use that data for direct marketing purposes provided that it has (a) obtained the relevant individual's consent for use of its personal data for those purposes; and (b) provided the individuals with a simple way to opt out of receiving direct marketing communications from the organization.</p> <p>In addition, APRA Prudential Standard CPS 234 - Information Security contains specific requirements on insurance companies towards taking a proactive approach in protecting all their data against cyber-security risks.</p>
 CHINA	<p>None.</p>
 HONG KONG	<p>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.</p>
 INDONESIA	<p>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 the processing, or the use, of the personal data by insurance companies.</p>
 JAPAN	<p>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 such third parties such as purpose of use, disclosure procedure and disclosure of inquiry or complaint counter.</p> <p>Business operators must also keep a record of the date when it received the personal data, a matter concerning the said confirmation and other matters prescribed by the rules of the PPC.</p>
 MALAYSIA	<p>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.</p>
 PHILIPPINES	<p>If an insurance company obtains personal data from its business partners, the parties are required to 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. 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.</p>




ARE THERE ANY SPECIFIC REQUIREMENTS FOR INSURANCE COMPANIES IN RELATION TO THE RECEIPT OF PERSONAL DATA FROM THEIR BUSINESS PARTNERS?

 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 (for example, business partners), insurance companies shall inform the data subject of: (a) the source of the personal data; (b) the name of the collector (that is, 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.
 THAILAND	There are no specific requirements. However, under 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 (detailed in question 5).
 VIETNAM	There are no special requirements. However, insurance companies must ensure that their business partners have obtained sufficient consent from data subjects to transfer personal data to them.





CAN INSURANCE COMPANIES TRANSFER THE PERSONAL DATA OF THEIR INSURANCE AGENTS OR INTERMEDIARIES TO OTHER SERVICE PROVIDERS, SUCH AS INVESTIGATION AGENTS OR DEBT COLLECTORS?

 AUSTRALIA	<p>Insurance companies may disclose personal data of their agents or intermediaries to other service providers if such transfer is the primary purpose for collection, or such transfer is a related secondary purpose and an individual may reasonably expect the insurance company to disclose their personal information to such third parties. It is advisable for insurance companies to make such uses of personal data clear in their privacy policies and collection notices. If an individual may not reasonably expect the transfer of their personal data in this way, then their consent must be obtained before doing so.</p>
 CHINA	<p>Yes, provided that: (a) such transfer is consistent with the notification given to data subjects and the consent obtained and (b) such transfer is compliant with the restrictions on cross-border personal data transfer.</p>
 HONG KONG	<p>Insurers should take reasonably practicable measures to ensure that staff, insurance agents, investigation agents and debt collectors with access to customers' personal data are trained in complying with requirements under the PDPO. Certain provisions can also be incorporated into relevant service contracts with investigation agents and debt collectors.</p>
 INDONESIA	<p>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.</p>
 JAPAN	<p>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).</p> <p>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.</p>
 MALAYSIA	<p>Yes, subject to the insurer having obtained the consent of the insurance agents or intermediaries.</p> <p>Please also refer to the response to question 6 relating to personal data processed by data processors.</p>
 PHILIPPINES	<p>There is no specific provision/restriction regarding this transfer.</p> <p>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 specific consent of the data subject. Moreover, if the sharing of the personal data by the PIC is for a "commercial purpose," as discussed above, the DPA requires that there be an express "data-sharing agreement" between the PIC and the third party to whom such data is shared. Such "data-sharing agreement" (a) must establish adequate safeguards for data privacy and security, and uphold rights of data subjects and (b) will be subject to review by the NPC, on the latter's initiative or upon complaint of a data subject. 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.</p>
 SINGAPORE	<p>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.</p>






CAN INSURANCE COMPANIES TRANSFER THE PERSONAL DATA OF THEIR INSURANCE AGENTS OR INTERMEDIARIES TO OTHER SERVICE PROVIDERS, SUCH AS INVESTIGATION AGENTS OR DEBT COLLECTORS?

 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 PDPL and mentioned above.
 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).
 VIETNAM	Yes, if the data subject has consented or as requested by the authorities.



ARE THERE ADDITIONAL REGULATORY REQUIREMENTS IMPOSED WITH RESPECT TO THE OUTSOURCING OF DATA PROCESSING TO THIRD-PARTY DATA PROCESSORS?

 AUSTRALIA	<p>Organizations that disclose personal data to third parties should ensure there are contractual or other means in place to protect the personal data. In case of a data breach incident, the outsourcing organization may be held liable together with the third-party provider.</p> <p>When outsourcing/offshoring data management responsibilities, APRA Prudential Standards, which deal specifically with this area, would apply to insurance companies who plan to outsource material business activities. The key requirements of the Prudential Standard are that an APRA-regulated institution must:</p> <ul style="list-style-type: none"> · Have a policy, approved by their board, relating to outsourcing of material business activities · Have sufficient monitoring processes in place to manage the outsourcing of material business activities · For all outsourcing of material business activities with third parties, have a legally binding agreement in place, unless otherwise agreed by APRA · Consult with APRA prior to entering into agreements to outsource material business activities to service providers that conduct their activities outside Australia · Notify APRA after entering into agreements to outsource material business activities.
 CHINA	<p>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.</p> <p>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.</p> <p>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.</p> <p>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).</p>
 HONG KONG	<p>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.</p>
 INDONESIA	<p>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.</p>







ARE THERE ADDITIONAL REGULATORY REQUIREMENTS IMPOSED WITH RESPECT TO THE OUTSOURCING OF DATA PROCESSING TO THIRD-PARTY DATA PROCESSORS?

 JAPAN	<p>Where a business operator entrusts the handling of personal data under its control, in whole or in part, to another party, such a 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.</p> <p>However, the business operator must exercise necessary and appropriate supervision over the subcontractor to ensure proper security management of the personal data.</p>
 MALAYSIA	<p>Please refer to the response to question 6 relating to personal data processed by data processors.</p> <p>Insurers are also required to comply with the applicable outsourcing policy document and Guidelines on Data Management and MIS Framework issued by BNM.</p>
 PHILIPPINES	<p>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, to 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.</p> <p>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.</p> <p>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.</p>
 SINGAPORE	<p>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.</p> <p>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 to assure itself that a potential third-party data processor is capable of complying with the provisions of the PDPA.</p>
 TAIWAN	<p>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 relevant information as required by PDPL and mentioned above.</p>






ARE THERE ADDITIONAL REGULATORY REQUIREMENTS IMPOSED WITH RESPECT TO THE OUTSOURCING OF DATA PROCESSING TO THIRD-PARTY DATA PROCESSORS?

 THAILAND	<p>Yes. A notification from the Office of Insurance Commission (OIC) mentions this issue. The outsourcing of data processing is permitted with notification and requires no prior approval from the OIC. However, the notification obligates an insurance company to issue an internal protocol to be followed by the outsourcing service provider.</p> <p>In addition, under PDPA, the data processor shall have the following duties:</p> <ol style="list-style-type: none">(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 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
 VIETNAM	<p>There are no additional regulatory requirements other than the general obligations regarding the collection, use and transfer of personal data (see question 5 above). In addition, if a third-party transfer happens while data processing is outsourced to third-party data processors, the data custodian must obtain the data subject's consent for the transfer.</p>

DO INSURANCE COMPANIES HAVE TO ENSURE THIRD PARTIES MEET CERTAIN STANDARDS IN OUTSOURCING PROCESSING TO THIRD PARTIES? ARE THERE ADDITIONAL SAFEGUARDS TO BE TAKEN?

 AUSTRALIA	<p>See response to question 16 above.</p> <p>APRA Standards applicable to insurance companies expect that a regulated entity would be able to demonstrate the following:</p> <ul style="list-style-type: none"> · Ability to continue operations and meet core obligations following a loss of services · Maintenance of the quality of critical or sensitive data · Compliance with legislative and prudential requirements · A lack of impediments (from jurisdictional hurdles or technical complications) to APRA being able to fulfill its duties as prudential regulator (including timely access to data in a usable form).
 CHINA	<p>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.</p> <p>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.</p>
 HONG KONG	<p>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, technical and operational expertise, etc., in the process of selecting the service provider.</p>
 INDONESIA	<p>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.</p>
 JAPAN	<p>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.</p>
 MALAYSIA	<p>Yes — please refer to our response to question 16.</p>






DO INSURANCE COMPANIES HAVE TO ENSURE THIRD PARTIES MEET CERTAIN STANDARDS IN OUTSOURCING PROCESSING TO THIRD PARTIES? ARE THERE ADDITIONAL SAFEGUARDS TO BE TAKEN?

 PHILIPPINES	<p>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.</p> <p>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.</p>
 SINGAPORE	<p>Yes. Note that the Monetary Authority of Singapore's Outsourcing Guidelines may apply to insurers regulated by MAS. Please refer to our response to question 16.</p> <p>Organizations should ensure that third parties are bound by appropriate obligations to guarantee compliance with the PDPA.</p>
 TAIWAN	<p>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 handling client disputes.</p>
 THAILAND	<p>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. Insurance companies are also required to issue a protocol to be followed by the outsourcer.</p>
 VIETNAM	<p>No regulations exist concerning outsourcing of personal data to third parties. The general obligations on the collection, use and transfer of personal data would apply (see question 5 above).</p>







Data retention

18. What is the data retention requirement?
19. Are there regulatory requirements to have local data centers and disaster recovery processes?







WHAT IS THE DATA RETENTION REQUIREMENT?

 AUSTRALIA	<p>There are no specific data retention requirements under Australian privacy law, though we note that organizations should only retain personal data for as long as it is required to be used for the primary purpose for which it was collected.</p>
 CHINA	<p>The Information Security Technology – Personal Information Security Specification (GB/T 35273-2017) 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 or de-identified. It should be noted that the specification is a recommended standard rather than a mandatory standard.</p> <p>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:</p> <ul style="list-style-type: none"> · 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. <p>Where its customers' identities or any of its transaction records are involved in a suspicious transaction activity that is under an anti-money laundering investigation, and such anti-money laundering investigation work 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.</p> <p>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.</p>
 HONG KONG	<p>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.</p>
 INDONESIA	<p>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.</p>
 JAPAN	<p>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.</p> <p>Under the insurance regulations, insurance companies are required to maintain certain reports and business forms for the statutory retention period.</p> <p>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.</p>






WHAT IS THE DATA RETENTION REQUIREMENT?

 MALAYSIA	<p>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 fulfill 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.</p>
 PHILIPPINES	<p>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.</p> <p>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, the purpose and other relevant information.</p>
 SINGAPORE	<p>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.</p> <p>Where there is no longer a need for an organization to retain personal data, it must take prompt action to ensure that it does not hold such personal data by ceasing to retain the documents containing personal data or removing the means by which the personal data may be associated with particular individuals (that is, anonymizing the data).</p>
 TAIWAN	<p>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.</p> <p>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.</p>
 THAILAND	<p>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.</p>
 VIETNAM	<p>In general, the data custodian must delete stored information upon 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 must notify the data subject of such deletion. General archiving regulations will apply.</p> <p>In addition, Vietnam has a data localization requirement. Under the Cybersecurity Law, domestic and foreign enterprises that: (a) provide services on the telecom network, the internet and value-added services on cyberspace in Vietnam; and (b) are involved in the collection, exploitation, analysis, or processing of (i) personal information, (ii) data about users' relationships or (iii) data generated by users in Vietnam must store such information within the territory of Vietnam for a period specified by the Vietnamese government.</p>

ARE THERE REGULATORY REQUIREMENTS TO HAVE LOCAL DATA CENTERS AND DISASTER RECOVERY PROCESSES?

	AUSTRALIA	<p>There are no requirements under Australian privacy law to have local data centers.</p> <p>While not a strict legal or regulatory requirement, OAIC guidelines and APRA Prudential Practice Guides indicate the importance of adequate disaster recovery processes as part of an organization's robust IT, cybersecurity and privacy management systems.</p>
	CHINA	<p>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 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.</p>
	HONG KONG	<p>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.</p> <p>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.</p> <p>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.</p>
	INDONESIA	<p>Insurance companies are required to store personal data within data centers and disaster recovery centers situated in Indonesia. Insurance companies can use third-party data center service providers.</p>
	JAPAN	<p>There are currently no regulatory requirements to have local data centers.</p> <p>Under the PPC and FSA Guidelines, insurance companies are required to have certain recovery measures.</p>
	MALAYSIA	<p>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.</p> <p>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.</p>







ARE THERE REGULATORY REQUIREMENTS TO HAVE LOCAL DATA CENTERS AND DISASTER RECOVERY PROCESSES?

 PHILIPPINES	<p>The DPA does not specifically require the establishment of local data centers in the Philippines. However, 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:</p> <ul style="list-style-type: none"> · 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.
 SINGAPORE	<p>The MAS Notice 127 on Technology Risk Management applicable to all insurance companies 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.</p> <p>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.</p>
 TAIWAN	<p>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. Please note that the FSC has not granted any approval for individual customers’/policyholders’ data to be stored outside Taiwan.</p> <p>In the event 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.</p>
 THAILAND	<p>There are no requirements to have local data centers and disaster recovery processes under PDPA. Insurance companies should, however, consider whether these are required as part of security measures.</p>
 VIETNAM	<p>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).</p> <p>Regarding disaster recovery processes, the Cybersecurity Law requires that service providers in cyberspace formulate/develop plans and solutions to promptly resolve cybersecurity incidents.</p>

Data breach management

20. What are the consequences of a data privacy breach? Is it a criminal offense? What is the penalty?
21. Is there a statutory obligation to disclose data breaches to regulators?
22. Is there a statutory obligation to disclose data breaches to data owners?
23. What are the statutory obligations to cooperate with regulators if there is a data breach?
24. Is there a publicly accessible cybersecurity assistance service, such as a computer emergency response team?
25. Are there additional consequences that apply in the event of a data privacy breach under cybersecurity laws?

WHAT ARE THE CONSEQUENCES OF A DATA PRIVACY BREACH? IS IT A CRIMINAL OFFENSE? WHAT IS THE PENALTY?

	AUSTRALIA	<p>The Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth) will require certain “eligible” data breaches to be notified to the OAIC and affected individuals in accordance with that Act.</p> <p>Failing to comply with the Privacy Amendment Act would be an “interference with the privacy of an individual,” which may amount to a breach of a civil penalty provision of the Privacy Act. The main consequences include the risk of a determination to pay compensation and also the risk of paying civil penalties of an amount up to AUD 2.1 million (for corporations) and AUD 420,000 (for individuals).</p>
	CHINA	<p>Violations of personal data protection provisions may lead to confiscation of illegal gain and a fine of up to 10 times the illegal gain or RMB 1 million (in case there is no illegal gain), and in serious cases, suspension of business or revocation of business license and fines of up to RMB 100,000 for responsible individuals.</p> <p>Unauthorized cross-border transfer of data may result in confiscation of illegal gain and a fine of up to RMB 500,000 as well as suspension of business or revocation of business license and a fine of up to RMB 100,000 for responsible individuals.</p> <p>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).</p>
	HONG KONG	<p>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.</p> <p>Contravention of an enforcement notice could result in a fine of HKD 50,000 and imprisonment for two years.</p>
	INDONESIA	<p>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.</p> <p>Further, insurance companies are required to notify the data owner of any data breach under Regulation 20. The notification must be done 14 days after the insurance companies know of the breach.</p> <p>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.</p>
	JAPAN	<p>Under the APPI, various offenses are subject to sentences of imprisonment (with labor) of not more than one year, or a fine for not more than JPY 500,000.</p>
	MALAYSIA	<p>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 or imprisonment for a term not exceeding two years or both.</p>

WHAT ARE THE CONSEQUENCES OF A DATA PRIVACY BREACH? IS IT A CRIMINAL OFFENSE? WHAT IS THE PENALTY?



PHILIPPINES

A violation or breach of the DPA will be penalized with a fine and/or imprisonment. The fine ranges from PHP 100,000 to PHP 4 million (approximately USD 2,000 to USD 80,000) with a period of imprisonment ranging from one (1) year to seven (7) years. For large-scale violations of the DPA, that is, those that harm, affect or involve the personal information of at least 100 persons, the maximum imposable penalty shall be imposed.

Furthermore, if the offender is a juridical person, its licenses may be ordered revoked while the responsible officers and persons who participated in or by their gross negligence, allowed the commission of the offense, may be penalized with a fine and imprisonment.

In the case of aliens, they may be deported without further proceedings after serving the penalties described.

If the offender is a public officer, he or she may suffer perpetual or temporary absolute disqualification from office, as well as other penalties as may be described in the Philippine Administrative Code.



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.

Breach of the key obligations of the PDPA is not a criminal offense.

However, do note that contravention of the Do Not Call provision is criminal in nature.




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:

- 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.

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.

A breach of the Do Not Call provision may lead to the imposition of fines up to SGD 10,000 per offense.

WHAT ARE THE CONSEQUENCES OF A DATA PRIVACY BREACH? IS IT A CRIMINAL OFFENSE? WHAT IS THE PENALTY?

 TAIWAN	<p>A data privacy breach, which may harm other people's rights, is a criminal offense.</p> <p>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.</p>
 THAILAND	<p>If the data controller or the data processor 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 1 year or a fine of up to THB 1 million (approximately USD 31,358), or both.</p>
 VIETNAM	<p>Criminal penalties will likely not apply unless the infringement constitutes interception or unauthorized access of a person's communications (mail, telephone, telegraphic). Violations may result in two years' imprisonment and additional fines of up to VND 20 million (approximately USD 1,000) per offense, or prohibition against holding certain positions for up to five years.</p> <p>Administrative penalties may apply. For example, in the network environment, a fine upward of VND 20 million (USD 1,000) can be imposed on the use of personal data of others without prior consent.</p> <p>Civil sanctions (for example, compensation) may apply if the data subject sues the data custodian.</p>

IS THERE A STATUTORY OBLIGATION TO DISCLOSE DATA BREACHES TO REGULATORS?



AUSTRALIA

Subject to certain exceptions, under the Privacy Act, entities that have reasonable grounds to suspect that an eligible data breach has occurred will be required to carry out a “reasonable and expeditious assessment” of the suspected data breach. The entity will need to take reasonable steps to ensure the assessment is completed within 30 days after it becomes aware of the suspected data breach.

If an entity has reasonable grounds to believe that an eligible data breach has occurred, it must promptly notify the affected individuals and OAIC. This will involve:

- Preparing a statement setting out the entity’s identity and contact details, a description of the breach, the kind of information concerned and recommendations about what the affected individuals should do in response
- Giving a copy of the statement to the Australian Information Commissioner
- If practicable, taking reasonable steps to notify the contents of the statement to each individual to whom the relevant information relates, or, if it is not practicable to do so, to the individuals who are “at risk” of serious harm from the breach. An entity might choose to notify a statement under the first option where it would require an unreasonable amount of resources to assess which affected individuals are “at risk” from an eligible data breach and which are not. On the other hand, the second option may be more practicable if an entity is able to ascertain with a high degree of confidence that only some particular individuals are “at risk” from the eligible data breach.

If none of the above methods is practicable, the entity must publish the statement on its website and take reasonable steps to publicize its content. Further, if a data breach has affected more than one entity, the entity who prepares the statement may include the identity and contact details of the other entities involved.

Additionally, APRA Prudential Standard CPS 234 - Information Security requires insurance companies to notify APRA within 72 hours of becoming aware of a security incident that has:

- Materially affected, or had the potential to material affect, financially or non-financially, the entity, or the interests of depositors, policyholders, beneficiaries, or other customers; or
- Been notified to other regulators, whether in Australia or overseas.

While data breaches are not specifically mentioned in the Prudential Standard, a data breach would be classified as a security incident that has materially affected an insurance company.








CHINA

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.





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.












IS THERE A STATUTORY OBLIGATION TO DISCLOSE DATA BREACHES TO REGULATORS?

 HONG KONG	<p>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.</p> <p>According to GL20, “cybersecurity incident” refers to an event that threatens the security of the system of an insurance company that 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.</p>
 INDONESIA	<p>No. However, there is an obligation for electronic system operators to report to law enforcement or a relevant government agency if there is any system failure or disruption to the system. This reporting must be done regardless of whether there is data breach.</p>
 JAPAN	<p>Under the Guidelines on Measures in Case of Leakage of Personal Data (PPC Notice No. 1 of 2017) (Leakage Guidelines), business operators are recommended to report certain data breaches such as leakage of personal data to the regulators promptly. Under the PPC and FSA Guidelines, insurance companies are required to report certain data breaches such as leakage of personal data to the regulators immediately.</p>
 MALAYSIA	<p>Statutory data breach reporting obligations may be imposed in the future, in view of the public consultation paper on Data Breach Notification that was issued in late 2018. For now, there is no express obligation to do so. However, the Regulator is likely to take into account the mitigating steps a data user took in order to determine whether there has been a breach of the Security Principle. 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 etc.</p> <p>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.</p>
 PHILIPPINES	<p>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:</p> <ul style="list-style-type: none"> · 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. <p>The notification shall include: (a) nature of breach; (b) sensitive personal information involved; and (c) measures taken by the PIC to address the breach.</p>









IS THERE A STATUTORY OBLIGATION TO DISCLOSE DATA BREACHES TO REGULATORS?

 SINGAPORE	<p>Depending on the nature of the data breach, relevant obligations under the MAS Guidelines on Outsourcing and/or the MAS Notice 127 on Technology Risk Management may be triggered. Under MAS Notice 127, an insurer is required to notify the MAS 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 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.</p> <p>Organizations are encouraged, as a form of good practice, to notify the PDPC, any relevant third parties and authorities.</p> <p>The PDPC has also informed that it will consider factors like notifications made by organizations or the lack of notification in determining whether an organization has reasonably protected the personal data under its control or possession.</p>
 TAIWAN	<p>In the event personal data is stolen, altered, damaged, destroyed or disclosed, insurance companies shall report such event to the FSC immediately.</p>
 THAILAND	<p>In case 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.</p>
 VIETNAM	<p>Under the Cybersecurity Law, service providers in cyberspace must notify the regulators (i.e., the Ministry of Public Security or the Ministry of Defence) of (i) cybersecurity incidents and (ii) leak, damage or loss of users' data.</p> <p>On a related note, insurers must report cyber incidents that they are unable to handle on their own to one or more of the following members of the incident response network: the network member responsible for incident response for that user (if any), the ISP that directly supplies internet services to the user, and/or the Vietnam Computer Emergency Response Team (VNCERT). For serious cyber incidents, insurers are required to report to VNCERT immediately. Serious incidents include those that occur on a large scale, spread quickly, threaten serious harm to computer and internet network systems, cause serious loss of information, or require substantial national or international resources to resolve.</p>




IS THERE A STATUTORY OBLIGATION TO DISCLOSE DATA BREACHES TO DATA OWNERS?

	AUSTRALIA	Yes; see response to question 21. The notification obligations require notification to be made to both the OAIC and affected individuals.
	CHINA	If personal information has been or may be divulged, damaged or lost, network operators shall inform users promptly. 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	The Leakage Guidelines stipulate and recommend promptly notifying data owners of certain data breaches, such as leakage of personal data, as a necessary measure for business operators. Under the PPC and FSA Guidelines, insurance companies are required to notify data owners of certain data breaches such as leakage of personal data promptly.
	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	No, but organizations are encouraged as a form of good practice to notify individuals if their personal data has been compromised. The PDPC has also informed that it will consider factors like notifications made by organizations or the lack of notification in determining whether an organization has reasonably protected the personal data under its control or possession. If the organization voluntarily disclosed the personal data breach to the PDPC as soon as it learned of the breach and cooperated with the PDPC in its investigations, this would also be taken as a mitigating factor in the calculation of a financial penalty (if applicable). The PDPC is currently reviewing the PDPA and is considering adopting a data breach notification requirement.
	TAIWAN	When personal data is stolen, disclosed, altered or violated in any way due to violations of PDPL, insurance companies shall inform the data subjects 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.










WHAT ARE THE STATUTORY OBLIGATIONS TO COOPERATE WITH REGULATORS IF THERE IS A DATA BREACH?

	AUSTRALIA	See response to question 21 above.
	CHINA	No specific statutory requirements apply, unless the data breach constitutes a cybersecurity incident. However, if there is a data breach, it would be reasonable to expect the insurance company to cooperate with CBIRC or other Chinese regulators if they so request.
	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, cooperation with the Regulator may be taken into account in determining compliance with the Security Principle.
	PHILIPPINES	Although there is no explicit requirement under the DPA to cooperate with the regulators, PICs are required to at least promptly notify the NPC and the affected data subjects of personal data breaches. Please refer to our response to question 21.
	SINGAPORE	<p>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.</p> <p>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.</p> <p>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:</p> <ul style="list-style-type: none"> · 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 thinks fit. <p>The MAS may also exercise its powers of regulation over the insurance company.</p>

WHAT ARE THE STATUTORY OBLIGATIONS TO COOPERATE WITH REGULATORS IF THERE IS A DATA BREACH?

 TAIWAN	In the event of a data breach, insurance companies are required to immediately report such an 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.
 VIETNAM	For service providers in cyberspace, the Cybersecurity Law sets out a general obligation to cooperate with and support the regulators in resolving cybersecurity issues.

IS THERE A PUBLICLY ACCESSIBLE CYBERSECURITY ASSISTANCE SERVICE, SUCH AS A COMPUTER EMERGENCY RESPONSE TEAM (CERT)?

	AUSTRALIA	The Australian Cyber Security Centre (ACSC) responds to cyber threats and incidents as Australia's CERT team. They provide a range of services, including a hotline, email support, technical guidance on mitigating cyber threats, incident response support and coordination, information sharing and capability building. Additionally, the ACSC provides a ReportCyber service that allows individuals, sole traders, and small and large businesses to report cybercrime incidents.
	CHINA	Currently, no.
	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 the Cyber999 computer security incident handling and response help center as well as the Cybersecurity Malaysia Cyber Threat Research Centre. MyCERT works closely with law enforcement agencies such as the police, Securities Commission and BNM.
	PHILIPPINES	While not exactly a "CERT," the NPC is 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 Criminal Investigation Bureau handles relevant matters in relation to cybercrime.

IS THERE A PUBLICLY ACCESSIBLE CYBERSECURITY ASSISTANCE SERVICE, SUCH AS A COMPUTER EMERGENCY RESPONSE TEAM (CERT)?



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 Electronic Transactions Development Agency (**ETDA**), an organization under the Thai Ministry of Digital Economy and Society.






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. As discussed under question 21, insurers are required to immediately report serious cyber incidents to VNCERT.

ARE THERE ADDITIONAL CONSEQUENCES THAT APPLY IN THE EVENT OF A DATA PRIVACY BREACH UNDER CYBERSECURITY LAWS?

 AUSTRALIA	No. The Privacy Amendment Act sets out the primary obligations that apply in the event of a data breach in Australia.
 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	No additional 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 and Cybersecurity Act, there are criminal penalties for cybercrime-related offenses (for example, unauthorized access to computer material, unauthorized modification of computer material, etc.) The Act has extra-territorial scope and applies to any person, whatever his/her nationality or citizenship, outside as well as within Singapore. It should also be noted that an organization that fails to employ reasonable measures to protect personal data may be liable to pay a fine not exceeding SGD 1 million under the PDPA.

ARE THERE ADDITIONAL CONSEQUENCES THAT APPLY IN THE EVENT OF A DATA PRIVACY BREACH UNDER CYBERSECURITY LAWS?

 TAIWAN	In general, 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 his computer protection, or taking advantage of the system loophole of such other, accesses his 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, etc. — the offenders will face criminal liabilities.
 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	No additional consequences apply in the event of a data privacy breach under cybersecurity laws. General consequences under question 20 will apply.

Baker McKenzie helps clients overcome the challenges of competing in the global economy.

We solve complex legal problems across borders and practice areas. Our unique culture, developed over 65 years, enables our 13,000 people to understand local markets and navigate multiple jurisdictions, working together as trusted colleagues and friends to instill confidence in our clients.

www.bakermckenzie.com

©2020 Baker McKenzie. All rights reserved. Baker & McKenzie International is a Swiss Verein with member law firms around the world. In accordance with the common terminology used in professional service organizations, reference to a "partner" means a person who is a partner, or equivalent, in such a law firm. Similarly, reference to an "office" means an office of any such law firm.

This may qualify as "Attorney Advertising" requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.